Metadefender Client Scan Report

Start Time: **2017/06/15 06:59:44 GMT**
Stop Time: **2017/06/15 07:06:12 GMT**
Total Files Processed: **1125**
Total Potentially Infected Files: **4**
Unknown Files: **3**
Clean Files: **1118**
Total IPs Scanned: **0**
Potentially Infected IPs Found: **0**
Clean IPs Found: **0**

Client version: **4.0.7.152**
Device MAC address: **98:DE:D0:BA:CF:B1**
IP Address: **10.12.94.248**
Device name: **SB4-12**
User name: **D77-IT**

Potentially Infected Files

PresentationFramework.Aero.ni.dll 2016/10/31 08:27:40 PM Suspicious
C:\Windows\assembly\NativeImages_v2.0.50727_64\PresentationFramewo#\bb604053360de7674549f34867678df0\PresentationFramework.Aero.ni.dll
SHA256: 0C7AADA2B58C6C22C4AECF8C93EA979BA745866E85B684D7A97DA018ED6F5F44
Threat Name: No threat name
AV Name: Antiy
AV Definition Date: 2016/10/20

Clean Engine Results:
AVG (AV Def: 2016/10/31)
Agnitum (AV Def: 2016/10/30)
Avira (AV Def: 2016/10/31)
BitDefender (AV Def: 2016/10/31)
CYREN (AV Def: 2016/10/31)
DrWebGateway (AV Def: 2016/10/31)
Emsisoft (AV Def: 2016/10/31)
F-secure (AV Def: 2016/10/31)
Fortinet (AV Def: 2016/10/31)
Ikarus (AV Def: 2016/10/31)
K7 (AV Def: 2016/10/31)
McAfee (AV Def: 2016/10/31)
NANOAV (AV Def: 2016/10/31)
QuickHeal (AV Def: 2016/10/31)
SUPERAntiSpyware (AV Def: 2016/10/31)
ThreatTrack (AV Def: 2016/10/31)
TrendMicro (AV Def: 2016/10/31)
VirITeXplorer (AV Def: 2016/10/31)
Xvirus (AV Def: 2016/10/30)
Zoner (AV Def: 2016/10/26)
AegisLab (AV Def: 2016/10/31)
Ahnlab (AV Def: 2016/10/31)
Baidu (AV Def: 2016/10/31)
ByteHero (AV Def: 2016/10/31)
ClamAV (AV Def: 2016/10/31)
ESET (AV Def: 2016/10/31)
F-prot (AV Def: 2016/10/31)
Filseclab (AV Def: 2016/10/31)
Hauri (AV Def: 2016/10/31)
Jiangmin (AV Def: 2016/10/31)
Lavasoft (AV Def: 2016/10/31)
Microsoft (AV Def: 2016/10/31)
Preventon (AV Def: 2016/10/31)
STOPzilla (AV Def: 2016/10/31)
Sophos (AV Def: 2016/10/31)
TotalDefense (AV Def: 2016/10/27)
TrendMicroHouseCall (AV Def: 2016/10/30)
VirusBlokAda (AV Def: 2016/10/31)
Zillya! (AV Def: 2016/10/31)
nProtect (AV Def: 2016/10/31)

WindowsFormsIntegration.ni.dll 2016/10/31 08:27:50 PM Suspicious
C:\Windows\assembly\NativeImages_v2.0.50727_64\WindowsFormsIntegra#\034ba2112f20385f2d559793597bec2d\WindowsFormsIntegration.ni.dll
SHA256: 2DE21D181C946E783C481C879C9EE45EA878972DA831B287FB5982871F370D1A
Threat Name: No threat name
AV Name: Antiy
AV Definition Date: 2016/10/20

Clean Engine Results:
AVG (AV Def: 2016/10/31)
Agnitum (AV Def: 2016/10/30)
Avira (AV Def: 2016/10/31)
BitDefender (AV Def: 2016/10/31)
CYREN (AV Def: 2016/10/31)
DrWebGateway (AV Def: 2016/10/31)
AegisLab (AV Def: 2016/10/31)
Ahnlab (AV Def: 2016/10/31)
Baidu (AV Def: 2016/10/31)
ByteHero (AV Def: 2016/10/31)
ClamAV (AV Def: 2016/10/31)
ESET (AV Def: 2016/10/31)

Emsisoft (AV Def: 2016/10/31)
F-secure (AV Def: 2016/10/31)
Fortinet (AV Def: 2016/10/31)
Ikarus (AV Def: 2016/10/31)
K7 (AV Def: 2016/10/31)
McAfee (AV Def: 2016/10/31)
NANOAV (AV Def: 2016/10/31)
QuickHeal (AV Def: 2016/10/31)
SUPERAntiSpyware (AV Def: 2016/10/31)
ThreatTrack (AV Def: 2016/10/31)
TrendMicro (AV Def: 2016/10/31)
VirITeXplorer (AV Def: 2016/10/31)
Xvirus (AV Def: 2016/10/30)
Zoner (AV Def: 2016/10/26)
F-prot (AV Def: 2016/10/31)
Filseclab (AV Def: 2016/10/31)
Hauri (AV Def: 2016/10/31)
Jiangmin (AV Def: 2016/10/31)
Lavasoft (AV Def: 2016/10/31)
Microsoft (AV Def: 2016/10/31)
Preventon (AV Def: 2016/10/31)
STOPzilla (AV Def: 2016/10/31)
Sophos (AV Def: 2016/10/31)
TotalDefense (AV Def: 2016/10/27)
TrendMicroHouseCall (AV Def: 2016/10/30)
VirusBlokAda (AV Def: 2016/10/31)
Zillya! (AV Def: 2016/10/31)
nProtect (AV Def: 2016/10/31)

Microsoft.WindowsAPICodePack.dll 2013/12/03 10:38:35 PM 1/40
C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\Microsoft.WindowsAPICodePack.dll
SHA256: 6063A932C627F231220746D1D12B099A6504C422E0E527DCAA0662791AA35FCD
Threat Name: Trojan.Win32.Mal.Gen.35134
AV Name: STOPzilla
AV Definition Date: 2013/12/02

Clean Engine Results:
AVG (AV Def: 2013/12/02)
Agnitum (AV Def: 2013/12/03)
Antiy (AV Def: 2013/12/03)
BitDefender (AV Def: 2013/12/03)
ClamWin (AV Def: 2013/11/30)
ESET (AV Def: 2013/12/03)
F-prot (AV Def: 2013/12/03)
Filseclab (AV Def: 2013/11/29)
GFI (AV Def: 2013/12/03)
Ikarus (AV Def: 2013/12/03)
K7 (AV Def: 2013/12/03)
Lavasoft (AV Def: 2013/12/03)
McAfee (AV Def: 2013/12/03)
NANO (AV Def: 2013/12/03)
QuickHeal (AV Def: 2013/12/03)
Sophos (AV Def: 2013/12/03)
TotalDefense (AV Def: 2013/12/02)
TrendMicroHouseCall (AV Def: 2013/12/02)
VirusBlokAda (AV Def: 2013/12/03)
nProtect (AV Def: 2013/12/02)
AegisLab (AV Def: 2013/12/03)
Ahnlab (AV Def: 2013/12/04)
Avira (AV Def: 2013/12/03)
ByteHero (AV Def: 2013/12/03)
Commtouch (AV Def: 2013/12/03)
Emsisoft (AV Def: 2013/12/03)
F-secure (AV Def: 2013/12/03)
Fortinet (AV Def: 2013/12/03)
Hauri (AV Def: 2013/12/04)
Jiangmin (AV Def: 2013/12/03)
Kingsoft (AV Def: 2013/12/03)
Malwarebytes (AV Def: 2013/12/03)
Microsoft (AV Def: 2013/12/03)
Norman (AV Def: 2013/12/03)
SUPERAntiSpyware (AV Def: 2013/12/03)
Systweak (AV Def: 2013/12/03)
TrendMicro (AV Def: 2013/12/02)
VirIT (AV Def: 2013/12/03)
Zillya! (AV Def: 2013/12/01)

Microsoft.WindowsAPICodePack.Shell.dll 2013/08/10 10:20:09 PM 1/40
C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\Microsoft.WindowsAPICodePack.Shell.dll
SHA256: A4366D4FD1DE446CDB4F101AFA9FDB7F04DA57F307E225CA5E86DBB1E8F96B9F
Threat Name: Trojan.Win32.Mal.Gen.35134
AV Name: STOPzilla
AV Definition Date: 2013/08/09

Clean Engine Results:
AVG (AV Def: 2013/08/09)
Ahnlab (AV Def: 2013/08/09)
Avira (AV Def: 2013/08/09)
ByteHero (AV Def: 2013/08/09)
Commtouch (AV Def: 2013/08/09)
Emsisoft (AV Def: 2013/08/07)
F-secure (AV Def: 2013/08/09)
Fortinet (AV Def: 2013/08/09)
Hauri (AV Def: 2013/08/10)
Jiangmin (AV Def: 2013/08/09)
Kingsoft (AV Def: 2013/08/10)
McAfee (AV Def: 2013/08/09)
NetGate (AV Def: 2013/08/09)
Preventon (AV Def: 2013/08/09)
Sophos (AV Def: 2013/08/09)
TTLivescan (AV Def: 2013/08/05)
TrendMicro (AV Def: 2013/08/08)
VirIT (AV Def: 2013/08/09)
Agnitum (AV Def: 2013/08/09)
Antiy (AV Def: 2013/08/09)
BitDefender (AV Def: 2013/08/09)
ClamWin (AV Def: 2013/08/09)
ESET (AV Def: 2013/08/09)
F-prot (AV Def: 2013/08/09)
Filseclab (AV Def: 2013/08/09)
GFI (AV Def: 2013/08/09)
Ikarus (AV Def: 2013/08/09)
K7 (AV Def: 2013/08/06)
Malwarebytes (AV Def: 2013/08/09)
NANO (AV Def: 2013/08/09)
Norman (AV Def: 2013/08/09)
QuickHeal (AV Def: 2013/08/09)
Systweak (AV Def: 2013/08/09)
TotalDefense (AV Def: 2013/08/09)
TrendMicroHouseCall (AV Def: 2013/08/08)
VirusBlokAda (AV Def: 2013/08/09)

Zillya! (AV Def: 2013/08/09)
Zoner (AV Def: 2013/08/09)
nProtect (AV Def: 2013/08/09)

Skipped Files

Metadefender-Client-Cloud_4.0.7.exe
Explanation: Exceeded archive file number
G:\diagnostika\Metadefender-Client-Cloud_4.0.7.exe

GPAPI.dll
Explanation: Not found
C:\Windows\SysWOW64\GPAPI.dll

rasman.dll
Explanation: Not found
C:\Windows\SysWOW64\rasman.dll

Operating Memory

[Potential Infection] C:\Windows\assembly\NativeImages_v2.0.50727_64\PresentationFramewo#\bb604053360de7674549f34867678df0\PresentationFramework.Aero.ni.dll
[Potential Infection] C:\Windows\assembly\NativeImages_v2.0.50727_64\WindowsFormsIntegra#\034ba2112f20385f2d559793597bec2d\WindowsFormsIntegration.ni.dll
[Potential Infection] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\Microsoft.WindowsAPICodePack.dll
[Potential Infection] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\Microsoft.WindowsAPICodePack.Shell.dll
[Potential Infection] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CCC.exe
[Clean] C:\Windows\system32\SPINF.dll
[Clean] C:\Windows\System32\lsass.exe
[Clean] C:\Windows\SysWOW64\wbem\wbemsvc.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\AEM.Plugin.Hotkeys.Shared.dll
[Clean] C:\Windows\System32\SearchFilterHost.exe
[Clean] C:\Windows\system32\ADVAPI32.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Foundation.Private.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Aspect.DeviceDFP.Graphics.Shared.dll
[Clean] C:\Windows\System32\services.exe
[Clean] C:\Windows\System32\wbem\unsecapp.exe
[Clean] C:\Windows\syswow64\kernel32.dll
[Clean] C:\Windows\SysWOW64\wsock32.dll
[Clean] C:\Windows\system32\svchost.exe
[Clean] C:\Windows\System32\NLSData0003.dll
[Clean] C:\Windows\system32\api-ms-win-downlevel-advapi32-l2-1-0.dll
[Clean] C:\Windows\System32\svchost.exe
[Clean] C:\Windows\system32\basesrv.DLL
[Clean] C:\Windows\system32\wbem\unsecapp.exe
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Aspect.AMDHome.Graphics.Runtime.dll
[Clean] C:\Windows\System32\smss.exe
[Clean] c:\windows\system32\bcrypt.dll
[Clean] c:\windows\system32\eappcfg.dll
[Clean] C:\Windows\System32\wininit.exe
[Clean] c:\program files\windows defender\MpClient.dll
[Clean] C:\Windows\system32\VSSAPI.DLL
[Clean] C:\Windows\system32\KERNELBASE.dll
[Clean] C:\Windows\System32\win32spl.dll
[Clean] C:\Windows\system32\csrss.exe
[Clean] C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE12\MSORES.DLL
[Clean] C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscoreei.dll
[Clean] C:\Windows\SYSTEM32\ntdll.dll
[Clean] C:\Windows\System32\lsm.exe

[Clean] C:\Windows\system32\SECURITY.DLL
[Clean] C:\Windows\system32\wiatrace.dll
[Clean] C:\Windows\system32\AEPIC.dll
[Clean] C:\Windows\System32\csrss.exe
[Clean] C:\Program Files (x86)\Intel\Intel(R) Rapid Storage Technology\IAStorIcon.exe
[Clean] C:\Windows\System32\firewallapi.dll
[Clean] C:\Windows\syswow64\CRYPTBASE.dll
[Clean] C:\Windows\System32\winlogon.exe
[Clean] C:\Program Files\CCleaner\CCleaner64.exe
[Clean] C:\Windows\system32\BROWCLI.DLL
[Clean] C:\Windows\System32\atiesrxx.exe
[Clean] C:\Windows\System32\atieclxx.exe
[Clean] C:\Program Files\Internet Explorer\ieproxy.dll
[Clean] C:\Windows\system32\mssprxy.dll
[Clean] C:\Windows\System32\spoolsv.exe
[Clean] C:\Program Files\ESET\ESET Endpoint Security\egui.exe
[Clean] C:\Windows\system32\wtsapi32.dll
[Clean] C:\Windows\system32\MSCTF.dll
[Clean] C:\Windows\system32\atiumd6a.dll
[Clean] C:\Windows\System32\taskhost.exe
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Aspect.UpdateNotification.Graphics.Dashboard.dll
[Clean] C:\Windows\SysWOW64\ieframe.dll
[Clean] C:\Windows\system32\POWRPROF.dll
[Clean] C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorjit.dll
[Clean] C:\Windows\assembly\NativeImages_v2.0.50727_64\System\4f09ec6588a5caaeb2f2810a272da071\System.ni.dll
[Clean] C:\Windows\system32\wbem\wbemcore.dll
[Clean] C:\Windows\system32\atieclxx.exe
[Clean] C:\Windows\system32\wdmaud.drv
[Clean] C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
[Clean] C:\Windows\System32\dwm.exe
[Clean] c:\windows\system32\UBPM.dll
[Clean] C:\Windows\syswow64\WLDAP32.dll
[Clean] C:\Windows\system32\USP10.dll
[Clean] c:\windows\system32\WUDFPlatform.dll
[Clean] c:\windows\system32\umpo.dll
[Clean] C:\Windows\system32\LPK.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Aspect.DeviceDFP.Graphics.Dashboard.dll
[Clean] C:\Windows\syswow64\SspiCli.dll
[Clean] C:\Windows\explorer.exe
[Clean] C:\Program Files\ESET\ESET Endpoint Security\x86\ekrn.exe
[Clean] C:\Program Files (x86)\Common Files\microsoft shared\VS7DEBUG\MDM.EXE
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Component.Runtime.Shared.Private.dll
[Clean] c:\windows\system32\nlaapi.dll
[Clean] c:\windows\system32\wpdbusenum.dll
[Clean] C:\Windows\system32\pcwum.DLL
[Clean] C:\Program Files (x86)\Netop\Netop School\Student\NHOSTSVC.EXE
[Clean] C:\Windows\System32\slc.dll
[Clean] C:\Windows\system32\msvcrt.dll
[Clean] C:\Windows\System32\Actioncenter.dll
[Clean] C:\Windows\SysWOW64\IPHLPAPI.DLL
[Clean] C:\Program Files (x86)\Google\Update\1.3.33.5\GoogleCrashHandler.exe
[Clean] C:\Windows\system32\pots.dll
[Clean] C:\Windows\SysWOW64\SXS.DLL
[Clean] C:\Windows\system32\USER32.dll
[Clean] C:\Windows\SysWOW64\wer.dll
[Clean] C:\Program Files (x86)\Google\Update\1.3.33.5\GoogleCrashHandler64.exe
[Clean] C:\Program Files (x86)\TP-LINK\TP-LINK Wireless Configuration Utility\TWCU.exe
[Clean] C:\Windows\system32\XmlLite.dll

[Clean] C:\Windows\WinSxS\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.6195_none_d09154e044272b9a\MSVCP80.dll
[Clean] C:\Program Files (x86)\Hewlett-Packard\OrderReminder\OrderReminder.exe
[Clean] C:\Program Files\Realtek\Audio\HDA\RAVCpl64.exe
[Clean] C:\Windows\System32\GWX\GWX.exe
[Clean] C:\Windows\System32\SearchIndexer.exe
[Clean] C:\Windows\system32\SensApi.dll
[Clean] C:\Program Files (x86)\Intel\Intel(R) Rapid Storage Technology\IAStorDataMgrSvc.exe
[Clean] C:\Windows\system32\spool\DRIVERS\x64\3\ZGDI.dll
[Clean] C:\Windows\system32\imagehlp.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\MOM.exe
[Clean] C:\Windows\system32\RESUTILS.DLL
[Clean] C:\Users\D77-IT\AppData\Roaming\Metadefender-Local\SSLEAY32.dll
[Clean] c:\windows\system32\WINSPOOL.DRV
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CCC.exe
[Clean] C:\Windows\System32\SearchProtocolHost.exe
[Clean] C:\Windows\Microsoft.NET\Framework64\v3.0\WPF\PresentationFontCache.exe
[Clean] C:\Windows\SysWOW64\api-ms-win-downlevel-shell32-l1-1-0.dll
[Clean] C:\Windows\SysWOW64\Wlanapi.dll
[Clean] C:\Windows\SYSTEM32\wow64win.dll
[Clean] C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\LMS\LMS.exe
[Clean] C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\UNS\UNS.exe
[Clean] C:\Program Files (x86)\Nero\Update\NASvc.exe
[Clean] C:\Windows\system32\RpcRtRemote.dll
[Clean] C:\Windows\syswow64\SHELL32.dll
[Clean] C:\Windows\SysWOW64\OLEACC.dll
[Clean] C:\Program Files\Windows Media Player\wmpnetwk.exe
[Clean] C:\Windows\syswow64\GDI32.dll
[Clean] C:\Windows\system32\NLAapi.dll
[Clean] C:\Windows\SysWOW64\WSCAPI.dll
[Clean] C:\Windows\System32\npmproxy.dll
[Clean] C:\Windows\System32\WUDFHost.exe
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Component.Dashboard.dll
[Clean] C:\Program Files\ESET\ESET Endpoint Security\x86\ekrnScan.dll
[Clean] C:\Windows\system32\AUDIOSES.DLL
[Clean] C:\Windows\system32\DEVOBJ.dll
[Clean] C:\Windows\system32\kernel32.dll
[Clean] C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE12\OGL.DLL
[Clean] C:\Windows\system32\OLEAUT32.dll
[Clean] C:\Windows\System32\WINSTA.dll
[Clean] C:\Windows\system32\qmgrprxy.dll
[Clean] c:\windows\system32\wlansvc.dll
[Clean] C:\Windows\SYSTEM32\sechost.dll
[Clean] C:\Windows\system32\IPHLPAPI.DLL
[Clean] C:\Windows\System32\devrtl.DLL
[Clean] C:\Windows\system32\VssTrace.DLL
[Clean] C:\Windows\assembly\NativeImages_v2.0.50727_32\IAStorUtil\2d982b3734c50b1d67ee1590b439bd1e\IAStorUtil.ni.dll
[Clean] c:\windows\system32\MMDevAPI.DLL
[Clean] c:\windows\system32\PROPSYS.dll
[Clean] C:\Windows\system32\FwpucInt.dll
[Clean] C:\Windows\system32\CRYPT32.dll
[Clean] C:\Windows\SysWOW64\EhStorShell.dll
[Clean] C:\Windows\system32\MSASN1.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\DEM.Graphics.I1010.dll
[Clean] C:\Windows\System32\DNSAPI.dll
[Clean] C:\Windows\syswow64\RPCRT4.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Aspect.DeviceLCD.Graphics.Shared.dll
[Clean] c:\windows\system32\dsrole.dll

[Clean] C:\Windows\syswow64\ole32.dll
[Clean] C:\Windows\system32\GPAPI.dll
[Clean] C:\Windows\system32\wbem\wbemess.dll
[Clean] C:\Windows\System32\fwpuclnt.dll
[Clean] C:\Windows\system32\RPCRT4.dll
[Clean] c:\windows\system32\AVRT.dll
[Clean] C:\Windows\system32\keyiso.dll
[Clean] C:\Windows\system32\msi.dll
[Clean] C:\Windows\system32\SHELL32.dll
[Clean] C:\Windows\system32\ole32.dll
[Clean] C:\Windows\system32\EhStorAPI.dll
[Clean] C:\Windows\system32\stobject.dll
[Clean] C:\Windows\system32\CLBCatQ.DLL
[Clean] C:\Windows\system32\IMM32.DLL
[Clean] c:\windows\system32\WLANMSM.DLL
[Clean] C:\Windows\system32\SHLWAPI.dll
[Clean] C:\Windows\system32\winhttp.dll
[Clean] c:\windows\system32\rpcepmap.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Aspect.DeviceProperty.Graphics.Shared.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Aspect.OverDrive5.Graphics.shared.dll
[Clean] C:\Windows\system32\GDI32.dll
[Clean] C:\Windows\system32\PortableDeviceTypes.dll
[Clean] c:\windows\system32\fwpuclnt.dll
[Clean] C:\Windows\system32\DNSAPI.dll
[Clean] C:\Windows\System32\CRYPTBASE.dll
[Clean] c:\windows\system32\wscsvc.dll
[Clean] c:\windows\system32\WLANSEC.dll
[Clean] c:\windows\system32\uxsms.dll
[Clean] C:\Windows\system32\WS2_32.dll
[Clean] C:\Windows\System32\usbmon.dll
[Clean] c:\windows\system32\mpssvc.dll
[Clean] C:\Windows\System32\WTSAPI32.dll
[Clean] C:\Windows\system32\taskschd.dll
[Clean] C:\Windows\system32\SspiCli.dll
[Clean] c:\windows\system32\WINHTTP.dll
[Clean] C:\Windows\system32\netutils.dll
[Clean] C:\Windows\System32\PROPSYS.dll
[Clean] C:\Users\D77-IT\AppData\Roaming\Metadefender-Local\MetadefenderApp.exe
[Clean] C:\Windows\WinSxS\x86_microsoft.vc80.atl_1fc8b3b9a1e18e3b_8.0.50727.6195_none_d1cb102c435421de\ATL80.DLL
[Clean] C:\Windows\system32\wdiasqmmodule.dll
[Clean] C:\Windows\system32\dhcpcsvc6.DLL
[Clean] C:\Windows\system32\cryptdll.dll
[Clean] c:\windows\system32\audiosrv.dll
[Clean] C:\Windows\system32\credui.dll
[Clean] C:\Windows\system32\NSI.dll
[Clean] c:\windows\system32\rpcss.dll
[Clean] C:\Windows\SysWOW64\srvcli.dll
[Clean] c:\windows\system32\wlgpclnt.dll
[Clean] c:\windows\system32\POWRPROF.dll
[Clean] C:\Windows\system32\cngaudit.dll
[Clean] C:\Windows\SysWOW64\ntshrui.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Aspect.DisplaysOptions.Graphics.Runtime.dll
[Clean] C:\Windows\system32\ksuser.dll
[Clean] C:\Windows\system32\SETUPAPI.dll
[Clean] C:\Windows\System32\wbem\WmiPrvSE.exe
[Clean] C:\Windows\system32\slc.dll
[Clean] c:\windows\system32\l2gpstore.dll
[Clean] C:\Windows\system32\CFGMGR32.dll

[Clean] C:\PROGRA~2\MICROS~1\Office12\WINWORD.EXE
[Clean] c:\windows\system32\sfc_os.dll
[Clean] C:\Windows\System32\wsdapi.dll
[Clean] C:\Windows\System32\SSPICLI.DLL
[Clean] C:\Windows\System32\SspiCli.dll
[Clean] C:\Windows\SYSTEM32\MSCOREE.DLL
[Clean] C:\Windows\system32\sfc_os.DLL
[Clean] C:\Windows\system32\drmv2clt.dll
[Clean] c:\windows\system32\bitsperf.dll
[Clean] C:\Windows\splwow64.exe
[Clean] c:\windows\system32\OneX.DLL
[Clean] C:\Windows\SysWOW64\api-ms-win-core-synch-l1-2-0.DLL
[Clean] c:\windows\system32\wlanutil.dll
[Clean] C:\Windows\system32\shfolder.dll
[Clean] C:\Windows\system32\radardt.dll
[Clean] c:\windows\system32\SYSNTFY.dll
[Clean] C:\Windows\System32\MMDevApi.dll
[Clean] C:\Windows\System32\credssp.dll
[Clean] c:\windows\system32\eappprxy.dll
[Clean] C:\Windows\system32\MMDevAPI.DLL
[Clean] c:\windows\system32\WinSCard.dll
[Clean] C:\Windows\SysWOW64\CRYPTSP.dll
[Clean] C:\Windows\system32\DUser.dll
[Clean] C:\Windows\system32\kerberos.DLL
[Clean] C:\Windows\system32\wdi.dll
[Clean] C:\Windows\system32\negoexts.DLL
[Clean] C:\Windows\System32\msxml6.dll
[Clean] C:\Windows\system32\oleacc.dll
[Clean] c:\windows\system32\AUTHZ.dll
[Clean] C:\Windows\WinSxS\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.23407_none_5c02a2f5a011f9be\gdiplus.dll
[Clean] c:\windows\system32\XmlLite.dll
[Clean] C:\Windows\System32\WINHTTP.dll
[Clean] C:\Windows\system32\wkscli.dll
[Clean] C:\Windows\System32\cryptdll.dll
[Clean] C:\Windows\System32\CRYPTSP.dll
[Clean] C:\Windows\system32\winsrv.DLL
[Clean] C:\Windows\system32\rsaenh.dll
[Clean] C:\Windows\system32\WINTRUST.dll
[Clean] C:\Windows\system32\SYNCENG.dll
[Clean] C:\Windows\System32\RpcRtRemote.dll
[Clean] C:\Windows\System32\VERSION.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Aspect.TransCode.Graphics.Runtime.dll
[Clean] C:\Windows\system32\version.dll
[Clean] C:\Windows\System32\SensApi.dll
[Clean] C:\Windows\system32\profapi.dll
[Clean] C:\Windows\system32\srvcli.dll
[Clean] C:\Windows\system32\rtutils.dll
[Clean] C:\Windows\System32\provsvc.dll
[Clean] C:\Windows\system32\netcfgx.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Caste.HydraVision.Runtime.dll
[Clean] C:\Program Files (x86)\Google\Chrome\Application\58.0.3029.110\chrome_elf.dll
[Clean] C:\Windows\system32\Secur32.dll
[Clean] C:\Windows\System32\secur32.dll
[Clean] c:\windows\system32\eapsvc.dll
[Clean] C:\Windows\syswow64\CRYPT32.dll
[Clean] C:\Windows\SysWOW64\DDRAW.dll
[Clean] c:\windows\system32\ssdpsrv.dll
[Clean] C:\Windows\system32\FVECERTS.dll

[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CCC.Implementation.dll
[Clean] C:\Windows\system32\umb.dll
[Clean] C:\Windows\system32\wbem\ncprov.dll
[Clean] c:\windows\system32\dhcpcsvc.DLL
[Clean] C:\Windows\System32\conhost.exe
[Clean] C:\Windows\System32\mswsock.dll
[Clean] C:\Users\D77-IT\AppData\Roaming\Metadefender-Local\x64\mdproxy.exe
[Clean] c:\windows\system32\IPHLPAPI.DLL
[Clean] C:\Windows\System32\rundll32.exe
[Clean] c:\windows\system32\pcasvc.dll
[Clean] C:\Windows\system32\DEVRTL.dll
[Clean] c:\windows\system32\AEPIC.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\APM.Server.dll
[Clean] c:\windows\system32\pcwum.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\AEM.Plugin.Source.Kit.Server.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Aspect.UpdateNotification.Graphics.Shared.dll
[Clean] c:\windows\system32\WINNSI.DLL
[Clean] C:\Windows\system32\eapphost.dll
[Clean] c:\windows\system32\sfc.dll
[Clean] C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{C9BB5A7D-84BE-4189-A630-00A205014E12}\mpengine.dll
[Clean] C:\Windows\system32\wiarpc.dll
[Clean] C:\Program Files (x86)\Nero\Update\NASvcPS.dll
[Clean] C:\Windows\System32\api-ms-win-downlevel-shell32-l1-1-0.dll
[Clean] C:\Windows\system32\USERENV.dll
[Clean] C:\Program Files (x86)\Intel\Intel(R) Rapid Storage Technology\ISDI.dll
[Clean] C:\Windows\system32\opengl32.dll
[Clean] C:\Windows\system32\api-ms-win-core-synch-l1-2-0.DLL
[Clean] C:\Windows\system32\apphelp.dll
[Clean] C:\Windows\SysWOW64\UIRibbon.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\AEM.Plugin.DPPE.Shared.dll
[Clean] C:\Windows\System32\webio.dll
[Clean] c:\windows\system32\VERSION.dll
[Clean] C:\Users\D77-IT\AppData\Roaming\Metadefender-Local\LIBEAY32.dll
[Clean] c:\windows\system32\wevtapi.dll
[Clean] C:\Program Files\ESET\ESET Endpoint Security\x86\ekrnAmon.dll
[Clean] C:\Windows\system32\rasman.dll
[Clean] c:\windows\system32\sysmain.dll
[Clean] C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Core\264f165cc1bbd95c43e92cb40f7be2c4\System.Core.ni.dll
[Clean] c:\windows\system32\trkwks.dll
[Clean] C:\Windows\System32\ntmarta.dll
[Clean] c:\windows\system32\ATL.DLL
[Clean] C:\Windows\system32\ncrypt.dll
[Clean] C:\Windows\system32\WLDAP32.dll
[Clean] C:\Windows\system32\wls0wndh.dll
[Clean] c:\windows\system32\netman.dll
[Clean] C:\Windows\system32\atiadlxx.dll
[Clean] C:\Windows\System32\netshell.dll
[Clean] C:\Windows\system32\SndVolSSO.DLL
[Clean] C:\Windows\System32\nlaapi.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\LOG.Foundation.dll
[Clean] C:\Windows\System32\RASDLG.dll
[Clean] C:\Windows\System32\MPRAPI.dll
[Clean] C:\Windows\system32\urlmon.dll
[Clean] c:\windows\system32\lmhsvc.dll
[Clean] C:\Windows\System32\rasadhlp.dll
[Clean] C:\Windows\system32\api-ms-win-downlevel-advapi32-l1-1-0.dll
[Clean] C:\Windows\System32\RASAPI32.dll

[Clean] c:\program files\windows defender\mpsvc.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Caste.Platform.Dashboard.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Aspect.CustomFormatSelection.Graphics.Dashboard.Shared.Private.dll
[Clean] C:\Windows\system32\wbem\wbemsvc.dll
[Clean] C:\Windows\System32\ncrypt.dll
[Clean] C:\Windows\System32\dhcpcsvc6.DLL
[Clean] C:\Windows\system32\wbem\fastprox.dll
[Clean] C:\Windows\system32\wbem\FastProx.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Foundation.dll
[Clean] C:\Windows\System32\rasman.dll
[Clean] C:\Windows\system32\UBPM.dll
[Clean] C:\Users\D77-IT\AppData\Roaming\Metadefender-Local\x64\libwadeviceinfo.dll
[Clean] c:\windows\system32\profsvc.dll
[Clean] C:\Windows\system32\NTDSAPI.dll
[Clean] C:\Windows\System32\rtutils.dll
[Clean] C:\Windows\SysWOW64\ATL.DLL
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Combined.Graphics.Aspects1.Dashboard.dll
[Clean] c:\windows\system32\hidserv.dll
[Clean] C:\Program Files (x86)\Common Files\Microsoft Shared\PROOF\MSSP3SK.DLL
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\DEM.Graphics.I0906.dll
[Clean] C:\Windows\system32\hnetcfg.dll
[Clean] C:\Windows\system32\ATL.DLL
[Clean] C:\Windows\system32\wbem\wbemprox.dll
[Clean] c:\windows\system32\HID.DLL
[Clean] C:\Windows\system32\wbemcomn.dll
[Clean] C:\Windows\system32\wbem\esscli.dll
[Clean] C:\Windows\syswow64\api-ms-win-downlevel-advapi32-l1-1-0.dll
[Clean] c:\windows\system32\wdi.dll
[Clean] C:\Windows\SysWOW64\VERSION.dll
[Clean] C:\Windows\System32\dskquota.dll
[Clean] C:\Program Files\ESET\ESET Endpoint Security\x86\ekrnHips.dll
[Clean] C:\Users\D77-IT\AppData\Roaming\Metadefender-Local\x64\libwaapi.dll
[Clean] C:\Windows\system32\dxp.dll
[Clean] C:\Windows\SYSTEM32\APPHLPDM.DLL
[Clean] C:\Windows\System32\wer.dll
[Clean] C:\Windows\system32\CRYPTSP.dll
[Clean] c:\windows\system32\es.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Aspect.DeviceProperty.Graphics.Runtime.dll
[Clean] C:\Windows\system32\rasadhlp.dll
[Clean] C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.18837_none_fa3b1e3d17594757\COMCTL32.dll
[Clean] C:\Windows\system32\PortableDeviceApi.dll
[Clean] C:\Windows\System32\NLSData000c.dll
[Clean] C:\Windows\system32\mswsock.dll
[Clean] C:\Windows\System32\portabledeviceconnectapi.dll
[Clean] c:\windows\system32\shsvcs.dll
[Clean] c:\windows\system32\nsisvc.dll
[Clean] c:\windows\system32\wudfsvc.dll
[Clean] C:\Windows\system32\SXS.DLL
[Clean] C:\Windows\system32\Normaliz.dll
[Clean] C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE11\msxml5.dll
[Clean] C:\Windows\system32\SAMCLI.DLL
[Clean] C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\UNS\xerces-c_2_7.dll
[Clean] C:\Windows\system32\rasapi32.dll
[Clean] c:\windows\system32\netprofm.dll
[Clean] C:\Windows\assembly\NativeImages_v2.0.50727_64\PresentationCore\46de1abdbafd8809843d5254e9ae2469\PresentationCore.ni.dll
[Clean] C:\Windows\system32\webio.dll

[Clean] C:\Windows\system32\CRYPTBASE.dll
[Clean] C:\Windows\SysWOW64\MSImg32.dll
[Clean] C:\Windows\system32\pcwum.dll
[Clean] C:\Windows\system32\credssp.dll
[Clean] C:\Windows\SysWOW64\IMM32.DLL
[Clean] C:\Windows\system32\WINNSI.DLL
[Clean] C:\Windows\system32\dhcpcsvc.DLL
[Clean] C:\Windows\System32\dhcpcore6.dll
[Clean] C:\Windows\system32\napinsp.dll
[Clean] C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscoreei.dll
[Clean] C:\Windows\system32\dwmapi.dll
[Clean] C:\Windows\system32\perftrack.dll
[Clean] C:\Windows\System32\FirewallAPI.dll
[Clean] c:\windows\system32\fntcache.dll
[Clean] C:\Windows\system32\wer.dll
[Clean] C:\Windows\System32\sfc_os.DLL
[Clean] C:\Windows\system32\sfc_os.dll
[Clean] C:\Windows\system32\PSAPI.DLL
[Clean] C:\Windows\syswow64\api-ms-win-downlevel-normaliz-l1-1-0.dll
[Clean] C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorwks.dll
[Clean] C:\Windows\system32\winspool.drv
[Clean] C:\Windows\system32\msctfui.dll
[Clean] C:\Windows\SysWOW64\cryptui.dll
[Clean] C:\Windows\system32\powertracker.dll
[Clean] C:\Windows\system32\VERSION.dll
[Clean] C:\Windows\system32\pnpts.dll
[Clean] C:\Windows\system32\pnrpnsp.dll
[Clean] C:\Windows\system32\WINHTTP.dll
[Clean] C:\Windows\system32\WINMM.dll
[Clean] C:\Windows\System32\winrnr.dll
[Clean] C:\Windows\system32\wpdshserviceobj.dll
[Clean] C:\Windows\System32\wshtcpip.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Aspect.Audio.Graphics.Dashboard.dll
[Clean] C:\Windows\system32\cryptbase.dll
[Clean] C:\Windows\SysWOW64\oledlg.dll
[Clean] C:\Windows\system32\wbem\wmiprov.dll
[Clean] C:\Windows\system32\elscore.dll
[Clean] C:\Windows\System32\wship6.dll
[Clean] C:\Windows\system32\WTSAPI32.dll
[Clean] C:\Windows\system32\pku2u.DLL
[Clean] C:\Program Files (x86)\Google\Chrome\Application\58.0.3029.110\chrome.dll
[Clean] C:\Windows\system32\OLEACC.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Component.Runtime.dll
[Clean] C:\Windows\syswow64\urlmon.dll
[Clean] C:\Windows\system32\HID.DLL
[Clean] C:\Program Files\CCleaner\lang\lang-1051.dll
[Clean] C:\Windows\system32\dbghelp.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Component.Dashboard.Shared.dll
[Clean] c:\windows\system32\webio.dll
[Clean] C:\Windows\system32\dwmredir.dll
[Clean] C:\Windows\system32\bcrypt.dll
[Clean] C:\Windows\System32\bcrypt.dll
[Clean] C:\Windows\system32\NETAPI32.dll
[Clean] C:\Windows\system32\lsm.exe
[Clean] C:\Windows\system32\SSPICLI.DLL
[Clean] C:\Windows\system32\scext.dll
[Clean] c:\windows\system32\qmgr.dll
[Clean] c:\windows\system32\gpsvc.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Aspect.DeviceDFP.Graphics.Runtime.dll

[Clean] C:\Windows\system32\DWrite.dll
[Clean] c:\windows\system32\schedsvc.dll
[Clean] c:\windows\system32\GPAPI.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\ATICCCom.dll
[Clean] c:\windows\system32\Secur32.dll
[Clean] c:\windows\system32\themeservice.dll
[Clean] C:\Windows\system32\OPENGL32.dll
[Clean] C:\Windows\system32\WINSTA.dll
[Clean] C:\Users\D77-IT\Desktop\android-studio-ide-171.4056697-windows\android-studio\jre\jre\bin\jawt.dll
[Clean] C:\Windows\system32\dsrole.dll
[Clean] c:\windows\system32\sens.dll
[Clean] C:\Windows\system32\SAMLIB.dll
[Clean] C:\Windows\system32\normaliz.DLL
[Clean] C:\Windows\system32\uxtheme.dll
[Clean] C:\Windows\system32\UxTheme.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\LOG.Foundation.Implementation.Private.dll
[Clean] C:\Windows\system32\ntmarta.dll
[Clean] c:\windows\system32\NETAPI32.dll
[Clean] C:\Windows\syswow64\IMM32.dll
[Clean] C:\Windows\system32\MsftEdit.dll
[Clean] c:\windows\system32\netutils.dll
[Clean] C:\Windows\system32\IconCodecService.dll
[Clean] C:\Windows\system32\FunDisc.dll
[Clean] c:\windows\system32\rtutils.dll
[Clean] C:\Windows\System32\wmpps.dll
[Clean] C:\Windows\System32\hcproviders.dll
[Clean] c:\windows\system32\srvcli.dll
[Clean] c:\windows\system32\wkscli.dll
[Clean] C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Web\e4288032a8c127c9c166ddea4ab3638b\Syste
m.Web.ni.dll
[Clean] C:\Windows\system32\PROPSYS.dll
[Clean] c:\windows\system32\ktmw32.dll
[Clean] C:\Windows\System32\WSDMon.dll
[Clean] C:\Windows\system32\tbs.dll
[Clean] C:\Windows\system32\wbem\wmiutils.dll
[Clean] C:\Windows\system32\FVEAPI.dll
[Clean] c:\windows\system32\iphlpsvc.dll
[Clean] C:\Windows\system32\LOGONCLI.DLL
[Clean] C:\Windows\system32\wbem\repdrvfs.dll
[Clean] C:\Program Files (x86)\Intel\Intel(R) Rapid Storage Technology\IAStorUIHelper.dll
[Clean] c:\windows\system32\FirewallAPI.dll
[Clean] C:\Windows\system32\bcryptprimitives.dll
[Clean] C:\Windows\system32\taskcomp.dll
[Clean] C:\Windows\syswow64\WINTRUST.dll
[Clean] C:\Windows\system32\ssdpapi.dll
[Clean] C:\Windows\system32\bitsigd.dll
[Clean] C:\Windows\syswow64\MSCTF.dll
[Clean] C:\Windows\system32\fwpuclnt.dll
[Clean] C:\Windows\System32\nlsp.dll
[Clean] C:\Windows\system32\samcli.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\DEM.Graphics.I0805.dll
[Clean] C:\Windows\system32\netjoin.dll
[Clean] C:\Windows\system32\mssph.dll
[Clean] c:\windows\system32\sqmapi.dll
[Clean] C:\Windows\SysWOW64\RpcRtRemote.dll
[Clean] C:\Windows\system32\api-ms-win-downlevel-shlwapi-l1-1-0.dll
[Clean] c:\windows\system32\nrpsrv.DLL
[Clean] c:\windows\system32\ikeext.dll
[Clean] C:\Windows\system32\SLC.dll

[Clean] C:\Windows\system32\SSCORE.DLL
[Clean] c:\windows\system32\WDSCORE.dll
[Clean] C:\Windows\System32\srvcli.dll
[Clean] c:\windows\system32\srvsvc.dll
[Clean] c:\windows\system32\wkssvc.dll
[Clean] c:\windows\system32\browser.dll
[Clean] C:\Users\D77-IT\AppData\Roaming\Metadefender-Local\x64\libwanetscan.dll
[Clean] c:\windows\system32\wbem\wmisvc.dll
[Clean] C:\Windows\system32\NCI.dll
[Clean] C:\Windows\syswow64\USERENV.dll
[Clean] C:\Windows\SysWOW64\wbem\wbemprox.dll
[Clean] C:\Windows\SysWOW64\WTSAPI32.DLL
[Clean] c:\windows\system32\DNSAPI.dll
[Clean] C:\Windows\System32\netprofm.dll
[Clean] C:\Windows\system32\CLUSAPI.DLL
[Clean] C:\Windows\WinSxS\x86_microsoft.vc90.crt_1fc8b3b9a1e18e3b_9.0.30729.4940_none_50916076bcb9a742\MSVCR90.dll
[Clean] C:\Windows\system32\devrtl.DLL
[Clean] C:\Windows\system32\wbem\wmiprvsd.dll
[Clean] C:\Windows\system32\ESENT.dll
[Clean] C:\Windows\syswow64\KERNEL32.dll
[Clean] C:\Windows\SysWOW64\wbemcomn.dll
[Clean] C:\Windows\system32\NCObjAPI.DLL
[Clean] C:\Windows\system32\atiu9p64.dll
[Clean] C:\Windows\system32\lsass.exe
[Clean] C:\Windows\system32\upnp.dll
[Clean] C:\Windows\syswow64\psapi.dll
[Clean] C:\Windows\syswow64\CFGMGR32.dll
[Clean] C:\Windows\System32\wscinterop.dll
[Clean] C:\Windows\system32\SSDPAPI.dll
[Clean] c:\windows\system32\aelupsvc.dll
[Clean] c:\windows\system32\appinfo.dll
[Clean] C:\Windows\SysWOW64\msi.dll
[Clean] C:\Windows\System32\NLSLexicons0013.dll
[Clean] c:\windows\system32\wuaueng.dll
[Clean] c:\windows\system32\ESENT.dll
[Clean] C:\Windows\System32\WMASF.DLL
[Clean] c:\windows\system32\Cabinet.dll
[Clean] c:\windows\system32\mspatcha.dll
[Clean] C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Configuration\55927dc9349959f3bb4a5002ab4a2715\System.Configuration.ni.dll
[Clean] C:\Windows\system32\psapi.dll
[Clean] C:\Windows\System32\NLSLexicons000c.dll
[Clean] C:\Windows\system32\WMsgAPI.dll
[Clean] C:\Windows\syswow64\KERNELBASE.dll
[Clean] C:\Windows\system32\SearchProtocolHost.exe
[Clean] C:\Windows\SysWOW64\wlanapi.dll
[Clean] C:\Windows\system32\dssenh.dll
[Clean] C:\Windows\syswow64\normaliz.DLL
[Clean] C:\Windows\System32\msxml3.dll
[Clean] C:\Windows\system32\cryptnet.dll
[Clean] c:\windows\system32\CRYPTNET.dll
[Clean] C:\Windows\system32\RasApi32.dll
[Clean] C:\Windows\system32\api-ms-win-downlevel-version-l1-1-0.dll
[Clean] C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\8a5ccf679e51f3a863c9951807a69f93\System.Windows.Forms.ni.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Aspect.UpdateNotification.Graphics.Runtime.dll
[Clean] C:\Windows\system32\SPPC.DLL

[Clean] C:\Windows\System32\snmpapi.dll
[Clean] C:\Program Files\ESET\ESET Endpoint Security\eguiAmon.dll
[Clean] C:\Windows\system32\sxs.dll
[Clean] c:\windows\system32\certprop.dll
[Clean] C:\Windows\system32\FXSAPI.dll
[Clean] C:\Windows\system32\schannel.DLL
[Clean] C:\Windows\system32\logoncli.dll
[Clean] C:\Windows\SYSTEM32\wow64.dll
[Clean] C:\Windows\SYSTEM32\wow64cpu.dll
[Clean] C:\Windows\syswow64\ADVAPI32.dll
[Clean] C:\Windows\system32\MFPlat.DLL
[Clean] C:\Windows\SysWOW64\WSOCK32.dll
[Clean] C:\Windows\SysWOW64\ntdll.dll
[Clean] C:\Windows\system32\IMM32.dll
[Clean] C:\Windows\syswow64\WS2_32.dll
[Clean] C:\Windows\SysWOW64\sechost.dll
[Clean] C:\Windows\SysWOW64\iphlpapi.dll
[Clean] C:\Windows\system32\MSSHooks.dll
[Clean] C:\Windows\syswow64\msvcrt.dll
[Clean] C:\Windows\System32\drivers\UMDF\WUDFUsbccidDriver.dll
[Clean] C:\Windows\syswow64\USER32.dll
[Clean] C:\Windows\syswow64\shell32.dll
[Clean] C:\Windows\system32\api-ms-win-downlevel-ole32-l1-1-0.dll
[Clean] C:\Windows\WinSxS\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_88df89932faf0bf6\MSVCR80.dll
[Clean] C:\Windows\syswow64\NSI.dll
[Clean] C:\Windows\WinSxS\amd64_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.23407_none_14556c1e8b95d0b8\gdiplus.dll
[Clean] C:\Windows\system32\wbem\cimwin32.dll
[Clean] c:\windows\system32\SspiCli.dll
[Clean] C:\Windows\syswow64\MSASN1.dll
[Clean] C:\Windows\system32\wdigest.DLL
[Clean] C:\Windows\system32\efslsaext.dll
[Clean] C:\Windows\syswow64\OLEAUT32.dll
[Clean] C:\Windows\syswow64\USP10.dll
[Clean] C:\Windows\SysWOW64\WINNSI.DLL
[Clean] C:\Windows\syswow64\LPK.dll
[Clean] C:\Windows\syswow64\SETUPAPI.dll
[Clean] C:\Windows\system32\sxssrv.DLL
[Clean] C:\Windows\system32\wininit.exe
[Clean] C:\Windows\system32\Cabinet.dll
[Clean] C:\Windows\system32\CRYPTUI.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Branding\Branding.dll
[Clean] C:\Windows\system32\secur32.dll
[Clean] C:\Windows\SysWOW64\webio.dll
[Clean] C:\Windows\SysWOW64\WINHTTP.dll
[Clean] c:\windows\system32\cryptsvc.dll
[Clean] C:\Windows\system32\AUTHZ.dll
[Clean] C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Drawing\82c506e2d08a2e538b4fa67c87bcdfa6\System.Drawing.ni.dll
[Clean] C:\Windows\system32\services.exe
[Clean] C:\Windows\system32\FirewallAPI.dll
[Clean] C:\Windows\system32\iertutil.dll
[Clean] C:\Windows\syswow64\DEVOBJ.dll
[Clean] C:\PROGRA~2\MICROS~1\Office12\wwlib.dll
[Clean] C:\Windows\system32\spool\DRIVERS\x64\3\ZSDNT5UI.DLL
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Aspect.DeviceCV.Graphics.Shared.dll
[Clean] C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\UNS\StatusStrings.dll
[Clean] C:\Windows\syswow64\SHLWAPI.dll

[Clean] C:\Users\D77-IT\AppData\Roaming\Metadefender-Local\x64\libwaheap.dll
[Clean] C:\Windows\system32\SspiSrv.dll
[Clean] C:\Windows\system32\explorerframe.dll
[Clean] C:\Windows\syswow64\profapi.dll
[Clean] C:\Windows\SysWOW64\rsaenh.dll
[Clean] C:\Windows\system32\api-ms-win-downlevel-normaliz-l1-1-0.dll
[Clean] C:\Windows\system32\SCESRV.dll
[Clean] C:\Windows\SysWOW64\MSCOREE.DLL
[Clean] C:\Windows\system32\wevtapi.dll
[Clean] C:\Windows\system32\SAMSRV.dll
[Clean] C:\Windows\system32\lsasrv.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\AEM.Server.dll
[Clean] C:\Windows\Microsoft.NET\Framework\v2.0.50727\diasymreader.dll
[Clean] C:\Windows\system32\wlanutil.dll
[Clean] C:\Windows\system32\msprivs.DLL
[Clean] C:\Windows\system32\Msidle.dll
[Clean] C:\Windows\syswow64\CLBCatQ.DLL
[Clean] C:\Windows\system32\thumbcache.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Aspect.DeviceTV.Graphics.shared.dll
[Clean] C:\Program Files\ESET\ESET Endpoint Security\x86\updater.dll
[Clean] C:\Windows\SYSTEM32\kernel32.dll
[Clean] C:\Windows\system32\dxgi.dll
[Clean] C:\Windows\System32\WUDFPlatform.dll
[Clean] C:\Windows\system32\MPR.dll
[Clean] C:\Windows\system32\CSRSRV.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\DEM.Graphics.I0703.dll
[Clean] C:\Windows\SysWOW64\sfc.dll
[Clean] c:\windows\system32\umpnpmgr.dll
[Clean] C:\Windows\SysWOW64\netutils.dll
[Clean] C:\Windows\SysWOW64\shdocvw.dll
[Clean] C:\Windows\system32\wmp.dll
[Clean] C:\Windows\system32\windowscodecs.dll
[Clean] c:\windows\system32\SPINF.dll
[Clean] C:\Windows\system32\atiumd64.dll
[Clean] C:\Windows\system32\netlogon.DLL
[Clean] C:\Windows\system32\msv1_0.DLL
[Clean] C:\Windows\WinSxS\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_88df89932faf0bf6\MSVCP80.dll
[Clean] c:\windows\system32\DEVRTL.dll
[Clean] C:\Windows\system32\scecli.DLL
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Component.Dashboard.ProfileManager2.dll
[Clean] C:\Windows\system32\tspkg.DLL
[Clean] C:\Windows\System32\AltTab.dll
[Clean] c:\windows\system32\WINSTA.dll
[Clean] C:\Windows\system32\SFC.DLL
[Clean] C:\Windows\system32\SYSNTFY.dll
[Clean] C:\Windows\system32\winlogon.exe
[Clean] C:\Windows\system32\wbem\wmidcprv.dll
[Clean] C:\Windows\System32\wkscli.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\DEM.Graphics.I0812.dll
[Clean] C:\Program Files\ESET\ESET Endpoint Security\eguiHips.dll
[Clean] C:\Windows\system32\UXINIT.dll
[Clean] C:\Windows\system32\WindowsCodecs.dll
[Clean] C:\Windows\system32\msiltcfg.dll
[Clean] C:\Windows\system32\atiesrxx.exe
[Clean] C:\Windows\system32\WINTRUST.DLL
[Clean] c:\windows\system32\dhcpcore.dll
[Clean] C:\Windows\SysWOW64\PROPSYS.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Combined.Graphics.Aspects2.Runtime.dll

[Clean] c:\windows\system32\wevtsvc.dll
[Clean] C:\Windows\System32\GPAPI.dll
[Clean] C:\Windows\System32\dhcpcsvc.DLL
[Clean] C:\Windows\System32\netutils.dll
[Clean] c:\windows\system32\dbghelp.dll
[Clean] C:\Windows\system32\MSVCR100.dll
[Clean] c:\windows\system32\dnsrslvr.dll
[Clean] C:\Windows\assembly\NativeImages_v2.0.50727_32\IsdiInterop\689ff5005671c420fe1ea3d7d2454667\IsdiInterop.ni.dll
[Clean] C:\Windows\System32\dnsext.dll
[Clean] C:\Windows\SysWOW64\wlanutil.dll
[Clean] C:\Windows\system32\wuapi.dll
[Clean] C:\Users\D77-IT\Desktop\android-studio-ide-171.4056697-windows\android-studio\bin\fsnotifier64.exe
[Clean] C:\Windows\system32\iphlpapi.dll
[Clean] C:\Windows\System32\NLSLexicons0027.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Aspect.DeviceCRT.Graphics.shared.dll
[Clean] c:\windows\system32\nlasvc.dll
[Clean] c:\windows\system32\netjoin.dll
[Clean] C:\Windows\system32\es.dll
[Clean] c:\windows\system32\ncsi.dll
[Clean] C:\Windows\system32\DDRAW.dll
[Clean] C:\Windows\system32\wbem\wmiprvse.exe
[Clean] C:\Windows\System32\POWRPROF.dll
[Clean] C:\Windows\System32\IPHLPAPI.DLL
[Clean] C:\Windows\System32\WINNSI.DLL
[Clean] C:\Windows\system32\SearchFilterHost.exe
[Clean] C:\Windows\System32\localspl.dll
[Clean] C:\Windows\System32\SPOOLSS.DLL
[Clean] C:\Program Files\Common Files\microsoft shared\ink\tiptsf.dll
[Clean] C:\Windows\System32\PrintIsolationProxy.dll
[Clean] C:\Windows\system32\WTSAPI32.DLL
[Clean] C:\Windows\System32\FXSMON.DLL
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Aspect.TransCode.Graphics.shared.dll
[Clean] C:\Windows\system32\spool\PRTPROCS\x64\winprint.dll
[Clean] C:\Windows\System32\NLSLexicons001b.dll
[Clean] C:\Windows\system32\fdPnp.dll
[Clean] C:\Windows\System32\tcpmon.dll
[Clean] C:\Windows\System32\dsrole.dll
[Clean] C:\Windows\system32\msls31.dll
[Clean] C:\Windows\SysWOW64\cscapi.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Aspect.MMVideo.Graphics.Shared.dll
[Clean] C:\Windows\System32\DEVRTL.dll
[Clean] C:\Windows\System32\wsnmp32.dll
[Clean] C:\Windows\System32\inetpp.dll
[Clean] C:\Windows\System32\webservices.dll
[Clean] C:\Windows\System32\SPINF.dll
[Clean] C:\Program Files\Windows Portable Devices\SqmApi.dll
[Clean] C:\Windows\system32\PresentationNative_v0300.dll
[Clean] C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Web\25433ee5d09d563da10280c1343511f9\System.Web.ni.dll
[Clean] C:\Windows\system32\uDWM.dll
[Clean] C:\Windows\System32\cscapi.dll
[Clean] C:\Users\D77-IT\Desktop\android-studio-ide-171.4056697-windows\android-studio\bin\studio64.exe
[Clean] c:\windows\system32\wsdapi.dll
[Clean] c:\windows\system32\bfe.dll
[Clean] c:\windows\system32\slc.dll
[Clean] C:\Windows\assembly\NativeImages_v2.0.50727_64\PresentationFramewo#\bf9feb78256176c1de6ea6ef4e8f299a\PresentationFramework.ni.dll
[Clean] C:\Windows\system32\wfapigp.dll

[Clean] c:\windows\system32\dps.dll
[Clean] C:\Windows\system32\shell32.dll
[Clean] C:\Windows\System32\wscapi.dll
[Clean] C:\Windows\System32\NLSLexicons001a.dll
[Clean] C:\Windows\System32\wercplsupport.dll
[Clean] C:\Windows\system32\diagperf.dll
[Clean] C:\Windows\system32\tdh.dll
[Clean] C:\Windows\system32\api-ms-win-downlevel-user32-l1-1-0.dll
[Clean] C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.18837_none_41e855142bd5705d\comctl32.dll
[Clean] C:\Windows\system32\dimsjob.dll
[Clean] C:\Program Files (x86)\TP-LINK\TP-LINK Wireless Configuration Utility\WJWF\WJWF_WPS_WIN7.DLL
[Clean] C:\Windows\system32\WININET.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\ADL.Foundation.dll
[Clean] C:\Program Files\ESET\ESET Endpoint Security\eguiParental.dll
[Clean] c:\windows\system32\diagtrack.dll
[Clean] c:\windows\system32\WTSAPI32.dll
[Clean] C:\Windows\SysWOW64\nlsp.dll
[Clean] C:\Program Files\ESET\ESET Endpoint Security\eguiDevmon.dll
[Clean] C:\Windows\system32\aepic.dll
[Clean] C:\Windows\System32\cryptnet.dll
[Clean] C:\Windows\system32\cscapi.dll
[Clean] C:\Windows\system32\DUI70.dll
[Clean] C:\Windows\System32\shacct.dll
[Clean] C:\Windows\system32\msimg32.dll
[Clean] C:\Program Files (x86)\Common Files\Microsoft Shared\VS7DEBUG\MDM.EXE
[Clean] C:\Windows\System32\bthprops.cpl
[Clean] C:\Windows\system32\MsCtfMonitor.dll
[Clean] C:\Windows\system32\syncui.dll
[Clean] C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.18837_none_41e855142bd5705d\COMCTL32.dll
[Clean] C:\Windows\system32\taskhost.exe
[Clean] C:\Windows\System32\XmlLite.dll
[Clean] C:\Windows\system32\MSUTB.dll
[Clean] C:\Windows\system32\sfc.dll
[Clean] C:\Windows\system32\shlwapi.DLL
[Clean] C:\Windows\SysWOW64\apphelp.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\LOG.Foundation.Private.dll
[Clean] C:\Windows\System32\tdh.dll
[Clean] C:\Windows\System32\PlaySndSrv.dll
[Clean] c:\program files\windows defender\mprtp.dll
[Clean] C:\Windows\AppPatch\AcWow64.DLL
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Caste.Fuel.Runtime.dll
[Clean] C:\Windows\system32\wininet.dll
[Clean] C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.18837_none_a4d981ff711297b6\COMCTL32.dll
[Clean] C:\Windows\system32\version.DLL
[Clean] C:\Windows\system32\AVRT.dll
[Clean] C:\Windows\SysWOW64\wtsapi32.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\DEM.Graphics.I0709.dll
[Clean] C:\Windows\SysWOW64\MSIMG32.dll
[Clean] C:\Windows\system32\TQUERY.DLL
[Clean] C:\Windows\system32\dwmcore.dll
[Clean] C:\Program Files\Internet Explorer\sqmapi.dll
[Clean] C:\Program Files\ESET\ESET Endpoint Security\MFC80U.DLL
[Clean] C:\Windows\SysWOW64\bcrypt.dll
[Clean] C:\Windows\system32\Dwm.exe
[Clean] C:\Windows\system32\d3d10_1.dll
[Clean] C:\Windows\system32\d3d10_1core.dll

[Clean] C:\Windows\syswow64\api-ms-win-downlevel-user32-l1-1-0.dll
[Clean] C:\Windows\system32\d3d11.dll
[Clean] C:\Windows\SysWOW64\NTDSAPI.dll
[Clean] C:\Users\D77-IT\Desktop\android-studio-ide-171.4056697-windows\android-studio\bin\focuskiller64.dll
[Clean] C:\Program Files\ESET\ESET Endpoint Security\eguiEmon.dll
[Clean] C:\Program Files\ESET\ESET Endpoint Security\eguiScan.dll
[Clean] C:\Program Files\ESET\ESET Endpoint Security\eguiDmon.dll
[Clean] C:\Program Files\ESET\ESET Endpoint Security\eguiEpfw.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Aspect.Radeon3D.Graphics.Dashboard.dll
[Clean] C:\Windows\system32\atiuxp64.dll
[Clean] C:\Windows\system32\aticfx64.dll
[Clean] C:\Windows\System32\SyncCenter.dll
[Clean] C:\Program Files\ESET\ESET Endpoint Security\eguiUpdate.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\APM.Foundation.dll
[Clean] C:\Program Files\ESET\ESET Endpoint Security\eguiSmon.dll
[Clean] C:\Windows\Explorer.EXE
[Clean] C:\Program Files (x86)\TP-LINK\TP-LINK Wireless Configuration Utility\nicLan.dll
[Clean] C:\Program Files\ESET\ESET Endpoint Security\shellExt.dll
[Clean] C:\Windows\system32\atidxx64.dll
[Clean] C:\Program Files\ESET\ESET Endpoint Security\eguiMailPlugins.dll
[Clean] C:\Windows\system32\EXPLORERFRAME.dll
[Clean] C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.18837_none_fa3b1e3d17594757\comctl32.dll
[Clean] C:\Windows\system32\EhStorShell.dll
[Clean] c:\windows\system32\fdrespub.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Aspect.DisplaysColour2.Graphics.Runtime.dll
[Clean] C:\Windows\SysWOW64\mpr.dll
[Clean] C:\Windows\system32\ntshrui.dll
[Clean] C:\Windows\system32\zipfldr.dll
[Clean] C:\Windows\system32\LINKINFO.dll
[Clean] C:\Users\D77-IT\Desktop\android-studio-ide-171.4056697-windows\android-studio\jre\jre\bin\server\jvm.dll
[Clean] C:\Windows\system32\msutb.dll
[Clean] C:\Windows\system32\actxprxy.dll
[Clean] C:\Windows\system32\timedate.cpl
[Clean] C:\Windows\System32\shdocvw.dll
[Clean] C:\Windows\System32\gameux.dll
[Clean] C:\Windows\System32\NLSLexicons0003.dll
[Clean] C:\Windows\system32\Wlanapi.dll
[Clean] C:\Windows\system32\fxsst.dll
[Clean] C:\Windows\system32\NetworkExplorer.dll
[Clean] C:\Windows\system32\BatMeter.dll
[Clean] C:\Windows\system32\FXSRESM.DLL
[Clean] C:\Windows\System32\UIAnimation.dll
[Clean] C:\Windows\system32\wwanapi.dll
[Clean] C:\Windows\system32\wwapi.dll
[Clean] C:\Windows\System32\QAgent.dll
[Clean] C:\Program Files (x86)\Common Files\Microsoft Shared\office12\riched20.dll
[Clean] C:\Windows\syswow64\iertutil.dll
[Clean] C:\Windows\system32\imapi2.dll
[Clean] C:\Windows\ehome\ehSSO.dll
[Clean] C:\Windows\System32\hgcpl.dll
[Clean] C:\Windows\syswow64\wintrust.dll
[Clean] C:\Windows\System32\NLSData0027.dll
[Clean] C:\Windows\SysWOW64\netapi32.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Caste.Graphics.Dashboard.dll
[Clean] C:\Windows\SysWOW64\samcli.dll
[Clean] C:\Windows\SysWOW64\wkscli.dll
[Clean] C:\Program Files (x86)\WinRAR\rarext64.dll
[Clean] C:\Windows\system32\wmdrmdev.dll

[Clean] C:\Windows\system32\SearchFolder.dll
[Clean] C:\Windows\system32\api-ms-win-downlevel-shlwapi-l2-1-0.dll
[Clean] C:\Windows\SysWOW64\rasapi32.dll
[Clean] C:\Windows\system32\prnfldr.dll
[Clean] C:\Windows\System32\WSCAPI.dll
[Clean] C:\Windows\system32\WINSPOOL.DRV
[Clean] C:\Windows\system32\Syncreg.dll
[Clean] C:\Program Files\ESET\ESET Endpoint Security\x86\ekrnEpfw.dll
[Clean] C:\Windows\system32\authui.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\AEM.Plugin.EEU.Shared.dll
[Clean] C:\Windows\System32\mshtml.dll
[Clean] C:\Windows\System32\wscui.cpl
[Clean] C:\Windows\System32\wevtapi.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\Localization.Foundation.Private.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Caste.Graphics.Dashboard.Shared.dll
[Clean] C:\Windows\System32\pnidui.dll
[Clean] C:\Windows\system32\DCIMAN32.dll
[Clean] C:\Windows\System32\werconcpl.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Aspect.MMVideo.Graphics.Dashboard.dll
[Clean] C:\Windows\SysWOW64\propsys.dll
[Clean] C:\Windows\System32\framedynos.dll
[Clean] C:\Windows\System32\StructuredQuery.dll
[Clean] C:\PROGRA~2\MICROS~1\Office12\GR469A~1.DLL
[Clean] C:\Windows\System32\srchadmin.dll
[Clean] C:\Windows\System32\QUtil.dll
[Clean] C:\Windows\system32\MLANG.dll
[Clean] C:\Windows\system32\twext.dll
[Clean] C:\Program Files\Common Files\Microsoft Shared\OFFICE11\msxml5.dll
[Clean] C:\Windows\SysWOW64\wscisvif.dll
[Clean] C:\Windows\system32\propsys.dll
[Clean] C:\Windows\syswow64\userenv.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\ResourceManagement.Foundation.Private.dll
[Clean] C:\Windows\syswow64\setupapi.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\AEM.Plugin.REG.Shared.dll
[Clean] C:\Windows\SysWOW64\faultrep.dll
[Clean] C:\Windows\syswow64\api-ms-win-downlevel-ole32-l1-1-0.dll
[Clean] C:\Windows\assembly\NativeImages_v2.0.50727_32\IAStorCommon\07cf963400f1454398a79308cd9ba191\IAStorCommon.ni.dll
[Clean] C:\Windows\System32\NLSData0000.dll
[Clean] C:\Windows\system32\wpdshext.dll
[Clean] C:\Windows\WinSxS\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.6195_none_d09154e044272b9a\MSVCR80.dll
[Clean] C:\Windows\System32\ieframe.dll
[Clean] C:\Windows\SysWOW64\ntmarta.dll
[Clean] C:\Windows\SysWOW64\secur32.dll
[Clean] C:\Windows\SysWOW64\schannel.dll
[Clean] C:\Windows\SysWOW64\dbghelp.dll
[Clean] C:\Windows\SysWOW64\credssp.dll
[Clean] C:\Windows\SysWOW64\wshtcpip.dll
[Clean] C:\Windows\SysWOW64\api-ms-win-downlevel-advapi32-l2-1-0.dll
[Clean] C:\Windows\syswow64\api-ms-win-downlevel-shlwapi-l1-1-0.dll
[Clean] C:\Windows\system32\WINBRAND.dll
[Clean] C:\Windows\syswow64\api-ms-win-downlevel-version-l1-1-0.dll
[Clean] C:\Windows\SysWOW64\rasadhlp.dll
[Clean] C:\Windows\SysWOW64\DNSAPI.dll
[Clean] C:\Program Files\ESET\ESET Endpoint Security\x86\ekrnEmon.dll
[Clean] C:\Windows\SysWOW64\version.DLL
[Clean] C:\Program Files\ESET\ESET Endpoint Security\x86\ekrnSmon.dll
[Clean] C:\Program Files\ESET\ESET Endpoint Security\x86\ekrnDmon.dll

[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Aspect.DisplaysOptions.Graphics.shared.dll
[Clean] C:\Windows\SysWOW64\rtutils.dll
[Clean] C:\Windows\System32\NLSData001b.dll
[Clean] C:\Program Files\ESET\ESET Endpoint Security\x86\ekrnUpdate.dll
[Clean] C:\Program Files\ESET\ESET Endpoint Security\x86\ekrnMailPlugins.dll
[Clean] C:\Program Files\ESET\ESET Endpoint Security\x86\ekrnParental.dll
[Clean] C:\Windows\assembly\NativeImages_v2.0.50727_32\System.ServiceProce#\311f6574141b35a4f4206f1f6da25a4b\System.ServiceProcess.ni.dll
[Clean] C:\Windows\SysWOW64\sfc_os.DLL
[Clean] C:\Windows\system32\GLU32.dll
[Clean] C:\Windows\system32\DSOUND.dll
[Clean] C:\Windows\SysWOW64\SCHEDCLI.DLL
[Clean] C:\Program Files\ESET\ESET Endpoint Security\x86\ekrnDevmon.dll
[Clean] C:\Windows\SysWOW64\fwpuclnt.dll
[Clean] C:\Windows\syswow64\wininet.dll
[Clean] C:\Windows\system32\COMDLG32.dll
[Clean] C:\Windows\SysWOW64\MPR.dll
[Clean] C:\Windows\system32\MSIMG32.dll
[Clean] C:\Windows\SysWOW64\hnetcfg.dll
[Clean] C:\Windows\System32\NaturalLanguage6.dll
[Clean] C:\Windows\system32\ElsLad.dll
[Clean] C:\Windows\system32\oledlg.dll
[Clean] C:\Windows\SysWOW64\uxtheme.dll
[Clean] C:\Windows\SysWOW64\wbem\fastprox.dll
[Clean] C:\Windows\SysWOW64\slc.dll
[Clean] C:\Windows\SysWOW64\dhcpcsvc.DLL
[Clean] C:\Windows\System32\NLSData0009.dll
[Clean] C:\Windows\SysWOW64\dwmapi.dll
[Clean] C:\Windows\System32\NLSLexicons0009.dll
[Clean] C:\Windows\SysWOW64\urlmon.dll
[Clean] C:\Program Files (x86)\TP-LINK\TP-LINK Wireless Configuration Utility\WJWF\WJWF.dll
[Clean] C:\Windows\syswow64\WININET.dll
[Clean] C:\Windows\System32\NLSData0007.dll
[Clean] C:\Windows\SysWOW64\dhcpcsvc6.DLL
[Clean] C:\Windows\SysWOW64\Secur32.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\DEM.Foundation.dll
[Clean] C:\Windows\SysWOW64\wship6.dll
[Clean] C:\Windows\SysWOW64\mswsock.dll
[Clean] C:\Windows\SysWOW64\NETAPI32.dll
[Clean] c:\windows\system32\wiaservc.dll
[Clean] c:\windows\system32\webservices.dll
[Clean] c:\windows\system32\scardsvr.dll
[Clean] C:\Windows\system32\HTTPAPI.dll
[Clean] C:\Windows\System32\NLSLexicons0007.dll
[Clean] C:\Windows\system32\SearchIndexer.exe
[Clean] C:\Windows\system32\MSSRCH.DLL
[Clean] C:\Windows\System32\NLSData001a.dll
[Clean] C:\Windows\System32\WUDFx.dll
[Clean] C:\Windows\System32\NLSData000a.dll
[Clean] C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll
[Clean] C:\Windows\AppPatch\AcSpecfc.DLL
[Clean] C:\Windows\System32\drivers\UMDF\WpdFs.dll
[Clean] C:\Windows\System32\wmvcore.dll
[Clean] C:\Windows\System32\portabledeviceclassextension.dll
[Clean] C:\Windows\system32\mscoree.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Caste.Graphics.Shared.dll
[Clean] C:\Windows\System32\NLSLexicons000a.dll
[Clean] C:\Windows\System32\NLSData0026.dll
[Clean] C:\Windows\assembly\NativeImages_v2.0.50727_32\mscorlib\38bf604432e1a30c954b2ee40d6a2d1c\mscorlib.ni.

dll
[Clean] C:\Windows\assembly\NativeImages_v2.0.50727_32\System\ef80bf7db724bb3ab5fea4c0e2117cae\System.ni.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\MOM.Foundation.dll
[Clean] C:\Windows\SysWOW64\CryptDll.dll
[Clean] C:\Windows\System32\NLSLexicons0026.dll
[Clean] C:\Windows\SysWOW64\qmgrprxy.dll
[Clean] C:\Windows\SysWOW64\Rstrtmgr.dll
[Clean] C:\Windows\SysWOW64\ncrypt.dll
[Clean] C:\Windows\System32\NLSData001d.dll
[Clean] C:\Windows\System32\NLSLexicons001d.dll
[Clean] C:\Windows\SysWOW64\msiltcfg.dll
[Clean] C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\ca97db61d7b1564dd115248a1439194e\System.Drawing.ni.dll
[Clean] C:\Windows\SysWOW64\SFC.DLL
[Clean] C:\Windows\System32\NLSData0013.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Caste.Platform.Shared.dll
[Clean] C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Xml\9b3962cac2f251a115ff3543d777007b\System.Xml.ni.dll
[Clean] C:\Windows\SysWOW64\shfolder.dll
[Clean] C:\Program Files (x86)\Intel\Intel(R) Rapid Storage Technology\IntelVisualDesign.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\AEM.Server.Shared.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\AEM.Plugin.WinMessages.Shared.dll
[Clean] C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Runtime.Remo#\48b76dbabfdec8c358f55380db91414c\System.Runtime.Remoting.ni.dll
[Clean] C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Xml\d6204638b750d650b7cbb3278a5954eb\System.Xml.ni.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Component.Runtime.Shared.dll
[Clean] C:\Windows\System32\NLSData0010.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Foundation.CoreAudioAPI.dll
[Clean] C:\Windows\System32\NLSLexicons0010.dll
[Clean] C:\Windows\syswow64\COMDLG32.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Aspect.AMDOverDrive.Platform.Dashboard.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Component.Client.Shared.dll
[Clean] C:\Windows\system32\ATIDEMGX.dll
[Clean] C:\Windows\assembly\NativeImages_v2.0.50727_32\WindowsBase\7a67eac9f95c5f0fe176f4612008c29f\WindowsBase.ni.dll
[Clean] C:\Windows\SysWOW64\UxTheme.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\DEM.Graphics.I0601.dll
[Clean] C:\Users\D77-IT\AppData\Roaming\Metadefender-Local\MSVCR120.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\Localization.Foundation.Implementation.default_Localization.dll
[Clean] C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Configuration\5271742225367c526b15a7c56eb9f751\System.Configuration.ni.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Caste.Graphics.Runtime.dll
[Clean] C:\Users\D77-IT\AppData\Roaming\Metadefender-Local\libcurl.dll
[Clean] C:\Windows\SysWOW64\WINSPOOL.DRV
[Clean] C:\Windows\SysWOW64\WINMM.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\AEM.Plugin.GD.Shared.dll
[Clean] C:\Windows\assembly\NativeImages_v2.0.50727_64\UIAutomationProvider\e96466ab3806d09e7ba5dc0ca5273544\UIAutomationProvider.ni.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Component.Runtime.Extension.EEU.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\atixclib.dll
[Clean] C:\Windows\system32\GWX\GWX.exe
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\DEM.Graphics.I0804.dll
[Clean] C:\Program Files (x86)\TP-LINK\TP-LINK Wireless Configuration Utility\DC_WFF.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\AEM.Actions.CCAA.Shared.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Aspect.AMDHome.Graphics.shared.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Aspect.HotkeysHandling.Graphics.Runtime.dll
[Clean] C:\Users\D77-IT\AppData\Roaming\Metadefender-Local\x64\libwainfection.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Aspect.HotkeysHandling.Graphics.Shared.dll

[Clean] C:\Windows\assembly\NativeImages_v2.0.50727_64\WindowsBase\77abbc5dbc24fe6d7695c70e1fccb79d\WindowsBase.ni.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Foundation.Client.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Caste.Graphics.Runtime.Shared.Private.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Aspect.DisplaysColour2.Graphics.Shared.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\DEM.Graphics.I0912.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Aspect.DeviceCRT.Graphics.Runtime.dll
[Clean] C:\Windows\assembly\NativeImages_v2.0.50727_32\IAStorDataMgrSvc\fbbda0031453de9f7c65c324d186bb76\IAStorDataMgrSvc.ni.exe
[Clean] C:\Windows\assembly\NativeImages_v2.0.50727_32\IAStorDataMgr\27dc9dcfd8b3fc13af5e1161f8c31bfe\IAStorDataMgr.ni.dll
[Clean] C:\Windows\SysWOW64\IconCodecService.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\DEM.Graphics.I0706.dll
[Clean] C:\Windows\Microsoft.NET\Framework64\v3.0\WPF\wpfgfx_v0300.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\DEM.Graphics.I1011.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Caste.Fuel.Shared.dll
[Clean] C:\Users\D77-IT\Desktop\android-studio-ide-171.4056697-windows\android-studio\jre\jre\bin\nio.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\DEM.Graphics.I0712.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Aspect.CustomFormats.Graphics.Shared.dll
[Clean] C:\Program Files (x86)\Intel\Intel(R) Rapid Storage Technology\IsdiInterop.dll
[Clean] C:\Windows\WinSxS\x86_microsoft.vc90.crt_1fc8b3b9a1e18e3b_9.0.30729.4940_none_50916076bcb9a742\msvcm90.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Caste.Platform.Runtime.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Aspect.AMDOverDrive.Platform.Runtime.dll
[Clean] C:\Windows\SysWOW64\WindowsCodecs.dll
[Clean] C:\Windows\system32\WSOCK32.dll
[Clean] C:\Windows\system32\KERNEL32.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\Fuel.Foundation.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Aspect.MMVideo.Graphics.Runtime.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Aspect.Radeon3D.Graphics.Shared.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Aspect.AMDOverDrive.Platform.Shared.dll
[Clean] C:\Windows\SysWOW64\MSFTEDIT.DLL
[Clean] C:\PROGRA~2\MICROS~1\Office12\GrooveNew.DLL
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Aspect.CPUOverDrive.Fuel.Shared.dll
[Clean] C:\Windows\SysWOW64\taskschd.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Component.Client.Shared.Private.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Caste.HydraVision.Shared.dll
[Clean] C:\Windows\SysWOW64\XmlLite.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Component.Dashboard.Shared.Private.dll
[Clean] C:\Windows\SysWOW64\api-ms-win-downlevel-shlwapi-l2-1-0.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Component.Systemtray.dll
[Clean] C:\PROGRA~2\MICROS~1\Office12\GrooveUtil.DLL
[Clean] C:\Windows\assembly\NativeImages_v2.0.50727_64\mscorlib\fe6ac93181b40a571892e14bfb9d65f2\mscorlib.ni.dll
[Clean] C:\Windows\SysWOW64\Winspool.DRV
[Clean] C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorjit.dll
[Clean] C:\Windows\system32\d3d9.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\ResourceManagement.Foundation.Implementation.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Foundation.XManifest.dll
[Clean] C:\Windows\SysWOW64\WINSTA.dll
[Clean] C:\Windows\system32\d3d8thk.dll
[Clean] C:\Program Files (x86)\Microsoft Office\Office12\msproof6.dll
[Clean] C:\Program Files (x86)\Microsoft Office\Office12\MSOSTYLE.DLL
[Clean] C:\PROGRA~2\MICROS~1\Office12\oart.dll
[Clean] C:\Windows\system32\spool\DRIVERS\x64\3\ZSDDM.DLL
[Clean] C:\Windows\system32\spool\DRIVERS\x64\3\ZSPOOL.dll
[Clean] C:\Windows\system32\wmploc.dll
[Clean] C:\Windows\Microsoft.Net\Framework64\v3.0\WPF\PresentationFontCache.exe
[Clean] C:\Windows\assembly\NativeImages_v2.0.50727_64\System.ServiceProce#\6f4eca98da0cd51e2f295988651bb0

93\System.ServiceProcess.ni.dll
[Clean] C:\Windows\system32\spool\DRIVERS\x64\3\ZTAG.dll
[Clean] C:\Windows\System32\WINUSB.DLL
[Clean] C:\Windows\system32\spool\DRIVERS\x64\3\ZSDDMUI.DLL
[Clean] C:\Users\D77-IT\Desktop\android-studio-ide-171.4056697-windows\android-studio\jre\jre\bin\zip.dll
[Clean] C:\Windows\system32\spool\DRIVERS\x64\3\ZSR.dll
[Clean] C:\Windows\system32\spool\DRIVERS\x64\3\ZIMFDRV.DLL
[Clean] C:\Users\D77-IT\Desktop\android-studio-ide-171.4056697-windows\android-studio\jre\jre\bin\java.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\MOM.Implementation.dll
[Clean] C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Windows.Forms\07db7a2abd633f1a43b3f65ad916bd91\System.Windows.Forms.ni.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Aspect.AMDHome.Graphics.Dashboard.dll
[Clean] C:\Users\D77-IT\Desktop\android-studio-ide-171.4056697-windows\android-studio\jre\jre\bin\net.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Aspect.Radeon3D.Graphics.Runtime.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\LOG.Foundation.Implementation.dll
[Clean] C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Runtime.Remo#\490290b7f83351b32a9fbc9820ca4ccc\System.Runtime.Remoting.ni.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Aspect.InfoCentre.Graphics.Dashboard.dll
[Clean] C:\Windows\system32\spool\DRIVERS\x64\3\ZIMF.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Aspect.CrossDisplay.Graphics.Dashboard.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Aspect.DisplaysManager.Graphics.Dashboard.dll
[Clean] C:\Windows\system32\framedynos.dll
[Clean] C:\Windows\SysWOW64\WTSAPI32.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\NEWAEM.Foundation.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Aspect.DisplaysOptions.Graphics.Dashboard.dll
[Clean] C:\Windows\system32\SECUR32.DLL
[Clean] C:\Windows\system32\NETAPI32.DLL
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Aspect.MultiVPU2.Graphics.Shared.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Aspect.OverDrive5.Graphics.Dashboard.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Aspect.TransCode.Graphics.Dashboard.dll
[Clean] C:\Windows\system32\SCHEDCLI.DLL
[Clean] C:\Windows\system32\WMI.DLL
[Clean] C:\Windows\system32\d2d1.dll
[Clean] C:\Windows\system32\DSROLE.DLL
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Caste.HydraVision.Dashboard.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Caste.Fuel.Dashboard.dll
[Clean] C:\Windows\system32\MAPI32.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\DEM.Graphics.dll
[Clean] C:\Users\D77-IT\Desktop\android-studio-ide-171.4056697-windows\android-studio\jre\jre\bin\freetype.dll
[Clean] C:\Windows\system32\mlang.dll
[Clean] C:\Users\D77-IT\.AndroidStudioPreview3.0\system\tmp\jna6865856742138392 45.dll
[Clean] C:\Users\D77-IT\Desktop\android-studio-ide-171.4056697-windows\android-studio\jre\jre\bin\fontmanager.dll
[Clean] C:\Users\D77-IT\Desktop\android-studio-ide-171.4056697-windows\android-studio\bin\IdeaWin64.dll
[Clean] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLI.Aspect.DeviceProperty.Graphics.Dashboard.Shared.dll
[Clean] C:\Users\D77-IT\Desktop\android-studio-ide-171.4056697-windows\android-studio\jre\jre\bin\management.dll
[Clean] C:\Users\D77-IT\Desktop\android-studio-ide-171.4056697-windows\android-studio\jre\jre\bin\sunmscapi.dll
[Clean] C:\Users\D77-IT\AppData\Roaming\Metadefender-Local\x64\LIBWAUTILS.dll
[Clean] C:\Windows\system32\FLTLIB.DLL
[Clean] C:\Users\D77-IT\AppData\Roaming\Metadefender-Local\x64\libwalocal.dll
[Clean] C:\Windows\AppPatch\AcGenral.DLL
[Clean] C:\Users\D77-IT\AppData\Roaming\Metadefender-Local\x64\libwaremoval.dll
[Clean] C:\Windows\system32\comdlg32.dll
[Clean] C:\Users\D77-IT\AppData\Roaming\Metadefender-Local\x64\libwacollector.dll
[Clean] C:\Users\D77-IT\AppData\Roaming\Metadefender-Local\x64\libwaaddon.dll
[Clean] C:\Users\D77-IT\AppData\Roaming\Metadefender-Local\x64\libwavmodapi.dll
[Clean] C:\Users\D77-IT\AppData\Roaming\Metadefender-Local\x64\libwaadbrowser.dll
[Clean] C:\Windows\system32\conhost.exe

[Clean] C:\Windows\SysWOW64\MSACM32.dll
[Clean] C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.18837_none_ec86b8d6858ec0bc\COMCTL32.dll
[Clean] C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.18837_none_41e855142bd5705d\Comctl32.dll
[Clean] C:\Windows\SysWOW64\mscms.dll
[Clean] C:\Windows\SysWOW64\DCIMAN32.dll
[Clean] C:\Program Files (x86)\Common Files\Microsoft Shared\office12\mso.dll
[Clean] C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE12\MSPTLS.DLL
[Clean] C:\Windows\SysWOW64\mscoree.dll
[Clean] C:\Users\D77-IT\Desktop\android-studio-ide-171.4056697-windows\android-studio\jre\jre\bin\sunec.dll
[Clean] C:\Users\D77-IT\Desktop\android-studio-ide-171.4056697-windows\android-studio\jre\jre\bin\awt.dll
[Clean] C:\PROGRA~2\MICROS~1\Office12\1051\wwintl.dll
[Clean] C:\Program Files (x86)\Common Files\Microsoft Shared\office12\1051\MSOINTL.DLL
[Clean] C:\Users\D77-IT\Desktop\android-studio-ide-171.4056697-windows\android-studio\jre\jre\bin\verify.dll

Installed Products

Internet Explorer 11.0.9600.18282 (update available)

CVE ID: CVE-2013-3893
Severity: CRITICAL
Description: Use-after-free vulnerability in the SetMouseCapture implementation in mshtml.dll in Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code via crafted JavaScript strings, as demonstrated by use of an ms-help: URL that triggers loading of hxds.dll.

CVE ID: CVE-2013-3897
Severity: CRITICAL
Description: Use-after-free vulnerability in the CDisplayPointer class in mshtml.dll in Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted JavaScript code that uses the onpropertychange event handler, as exploited in the wild in September and October 2013, aka "Internet Explorer Memory Corruption Vulnerability."

CVE ID: CVE-2013-3915
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2013-3917.

CVE ID: CVE-2013-3917
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2013-3915.

CVE ID: CVE-2013-5047
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2013-5048.

CVE ID: CVE-2013-5048
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2013-5047.

CVE ID: CVE-2013-7331
Severity: MODERATE
Description: The Microsoft.XMLDOM ActiveX control in Microsoft Windows 8.1 and earlier allows remote attackers to determine the existence of local pathnames, UNC share pathnames, intranet hostnames, and intranet IP addresses by examining error codes, as demonstrated by a res:// URL, and exploited in the wild in February 2014.

CVE ID: CVE-2014-0271
Severity: CRITICAL

Description: The VBScript engine in Microsoft Internet Explorer 6 through 11, and VBScript 5.6 through 5.8, allows r emote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "VBScript Memory Corruption Vulnerability."

CVE ID: CVE-2014-0275
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-0285 and CVE-2014-0286.

CVE ID: CVE-2014-0282
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-1775, CVE-2014-1779, CVE-2014-1799, CVE-2014 -1803, and CVE-2014-2757.

CVE ID: CVE-2014-0285
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-0275 and CVE-2014-0286.

CVE ID: CVE-2014-0286
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-0275 and CVE-2014-0285.

CVE ID: CVE-2014-0299
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-0305 and CVE-2014-0311.

CVE ID: CVE-2014-0305
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-0299 and CVE-2014-0311.

CVE ID: CVE-2014-0310
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-1815.

CVE ID: CVE-2014-0311
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-0299 and CVE-2014-0305.

CVE ID: CVE-2014-1762
Severity: IMPORTANT
Description: Unspecified vulnerability in Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code with medium-integrity privileges and bypass a sandbox protection mechanism via unknow n vectors, as demonstrated by ZDI during a Pwn4Fun competition at CanSecWest 2014.

CVE ID: CVE-2014-1765
Severity: IMPORTANT
Description: Multiple use-after-free vulnerabilities in Microsoft Internet Explorer 6 through 11 allow remote attackers to execute arbitrary code via unspecified vectors, as demonstrated by Sebastian Apelt and Andreas Sch midt during a Pwn2Own competition at CanSecWest 2014.

CVE ID: CVE-2014-1770
Severity: CRITICAL
Description: Use-after-free vulnerability in Microsoft Internet Explorer 6 through 11 allows remote attackers to execut

e arbitrary code via crafted JavaScript code that interacts improperly with a CollectGarbage function call on a CMarkup object allocated by the CMarkup::CreateInitialMarkup function.

CVE ID: CVE-2014-1771
Severity: IMPORTANT
Description: SChannel in Microsoft Internet Explorer 6 through 11 does not ensure that a server's X.509 certificate is the same during renegotiation as it was before renegotiation, which allows man-in-the-middle attackers t o obtain sensitive information or modify TLS session data via a "triple handshake attack," aka "TLS Serv er Certificate Renegotiation Vulnerability."

CVE ID: CVE-2014-1775
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-0282, CVE-2014-1779, CVE-2014-1799, CVE-2014 -1803, and CVE-2014-2757.

CVE ID: CVE-2014-1776
Severity: CRITICAL
Description: Use-after-free vulnerability in Microsoft Internet Explorer 6 through 11 allows remote attackers to execut e arbitrary code or cause a denial of service (memory corruption) via vectors related to the CMarkup::Is ConnectedToPrimaryMarkup function, as exploited in the wild in April 2014. NOTE: this issue originally emphasized VGX.DLL, but Microsoft clarified that "VGX.DLL does not contain the vulnerable code lever aged in this exploit. Disabling VGX.DLL is an exploit-specific workaround that provides an immediate, ef fective workaround to help block known attacks."

CVE ID: CVE-2014-1779
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-0282, CVE-2014-1775, CVE-2014-1799, CVE-2014 -1803, and CVE-2014-2757.

CVE ID: CVE-2014-1796
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 and 8 through 11 allows remote attackers to execute arbitrary code or cau se a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corrupt ion Vulnerability."

CVE ID: CVE-2014-1799
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-0282, CVE-2014-1775, CVE-2014-1779, CVE-2014 -1803, and CVE-2014-2757.

CVE ID: CVE-2014-1803
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-0282, CVE-2014-1775, CVE-2014-1779, CVE-2014 -1799, and CVE-2014-2757.

CVE ID: CVE-2014-1815
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, as exploited in the wild in May 2014, aka "Int ernet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-0310.

CVE ID: CVE-2014-2757
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-0282, CVE-2014-1775, CVE-2014-1779, CVE-2014 -1799, and CVE-2014-1803.

CVE ID: CVE-2014-2774
Severity: CRITICAL

Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-2820, CVE-2014-2826, CVE-2014-2827, and CVE-2014-4063.

CVE ID: CVE-2014-2799
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-4059, CVE-2014-4065, CVE-2014-4079, CVE-2014-4081, CVE-2014-4083, CVE-2014-4085, CVE-2014-4088, CVE-2014-4090, CVE-2014-4094, CVE-2014-4097, CVE-2014-4100, CVE-2014-4103, CVE-2014-4104, CVE-2014-4105, CVE-2014-4106, CVE-2014-4107, CVE-2014-4108, CVE-2014-4109, CVE-2014-4110, and CVE-2014-4111.

CVE ID: CVE-2014-2800
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-2807 and CVE-2014-2809.

CVE ID: CVE-2014-2807
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-2800 and CVE-2014-2809.

CVE ID: CVE-2014-2809
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-2800 and CVE-2014-2807.

CVE ID: CVE-2014-2817
Severity: IMPORTANT
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to gain privileges via a crafted web sit e, aka "Internet Explorer Elevation of Privilege Vulnerability."

CVE ID: CVE-2014-2820
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-2774, CVE-2014-2826, CVE-2014-2827, and CVE-2014-4063.

CVE ID: CVE-2014-2826
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-2774, CVE-2014-2820, CVE-2014-2827, and CVE-2014-4063.

CVE ID: CVE-2014-2827
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-2774, CVE-2014-2820, CVE-2014-2826, and CVE-2014-4063.

CVE ID: CVE-2014-4059
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-2799, CVE-2014-4065, CVE-2014-4079, CVE-2014-4081, CVE-2014-4083, CVE-2014-4085, CVE-2014-4088, CVE-2014-4090, CVE-2014-4094, CVE-2014-4097, CVE-2014-4100, CVE-2014-4103, CVE-2014-4104, CVE-2014-4105, CVE-2014-4106, CVE-2014-4107, CVE-2014-4108, CVE-2014-4109, CVE-2014-4110, and CVE-2014-4111.

CVE ID: CVE-2014-4063

Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-2774, CVE-2014-2820, CVE-2014-2826, and CVE-2014-2827.

CVE ID: CVE-2014-4065
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-2799, CVE-2014-4059, CVE-2014-4079, CVE-2014-4081, CVE-2014-4083, CVE-2014-4085, CVE-2014-4088, CVE-2014-4090, CVE-2014-4094, CVE-2014-4097, CVE-2014-4100, CVE-2014-4103, CVE-2014-4104, CVE-2014-4105, CVE-2014-4106, CVE-2014-4107, CVE-2014-4108, CVE-2014-4109, CVE-2014-4110, and CVE-2014-4111.

CVE ID: CVE-2014-4079
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-2799, CVE-2014-4059, CVE-2014-4065, CVE-2014-4081, CVE-2014-4083, CVE-2014-4085, CVE-2014-4088, CVE-2014-4090, CVE-2014-4094, CVE-2014-4097, CVE-2014-4100, CVE-2014-4103, CVE-2014-4104, CVE-2014-4105, CVE-2014-4106, CVE-2014-4107, CVE-2014-4108, CVE-2014-4109, CVE-2014-4110, and CVE-2014-4111.

CVE ID: CVE-2014-4081
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-2799, CVE-2014-4059, CVE-2014-4065, CVE-2014-4079, CVE-2014-4083, CVE-2014-4085, CVE-2014-4088, CVE-2014-4090, CVE-2014-4094, CVE-2014-4097, CVE-2014-4100, CVE-2014-4103, CVE-2014-4104, CVE-2014-4105, CVE-2014-4106, CVE-2014-4107, CVE-2014-4108, CVE-2014-4109, CVE-2014-4110, and CVE-2014-4111.

CVE ID: CVE-2014-4083
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-2799, CVE-2014-4059, CVE-2014-4065, CVE-2014-4079, CVE-2014-4081, CVE-2014-4085, CVE-2014-4088, CVE-2014-4090, CVE-2014-4094, CVE-2014-4097, CVE-2014-4100, CVE-2014-4103, CVE-2014-4104, CVE-2014-4105, CVE-2014-4106, CVE-2014-4107, CVE-2014-4108, CVE-2014-4109, CVE-2014-4110, and CVE-2014-4111.

CVE ID: CVE-2014-4085
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-2799, CVE-2014-4059, CVE-2014-4065, CVE-2014-4079, CVE-2014-4081, CVE-2014-4083, CVE-2014-4088, CVE-2014-4090, CVE-2014-4094, CVE-2014-4097, CVE-2014-4100, CVE-2014-4103, CVE-2014-4104, CVE-2014-4105, CVE-2014-4106, CVE-2014-4107, CVE-2014-4108, CVE-2014-4109, CVE-2014-4110, and CVE-2014-4111.

CVE ID: CVE-2014-4088
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-2799, CVE-2014-4059, CVE-2014-4065, CVE-2014-4079, CVE-2014-4081, CVE-2014-4083, CVE-2014-4085, CVE-2014-4090, CVE-2014-4094, CVE-2014-4097, CVE-2014-4100, CVE-2014-4103, CVE-2014-4104, CVE-2014-4105, CVE-2014-4106, CVE-2014-4107, CVE-2014-4108, CVE-2014-4109, CVE-2014-4110, and CVE-2014-4111.

CVE ID: CVE-2014-4090
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-2799, CVE-2014-4059, CVE-2014-4065, CVE-2014-4079, CVE-2014-4081, CVE-2014-4083, CVE-2014-4085, CVE-2014-4088, CVE-2014-4094, CVE-2014-4097, CVE-2014-4100, CVE-2014-4103, CVE-2014-4104, CVE-2014-4105, CVE-2014-4106, CVE-2014-4107, CVE-2014-4108, CVE-2014-4109, CVE-2014-4110, and CVE-2014-4111.

CVE ID: CVE-2014-4094

Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-2799, CVE-2014-4059, CVE-2014-4065, CVE-2014-4079, CVE-2014-4081, CVE-2014-4083, CVE-2014-4085, CVE-2014-4088, CVE-2014-4090, CVE-2014-4097, CVE-2014-4100, CVE-2014-4103, CVE-2014-4104, CVE-2014-4105, CVE-2014-4106, CVE-2014-4107, CVE-2014-4108, CVE-2014-4109, CVE-2014-4110, and CVE-2014-4111.

CVE ID: CVE-2014-4097
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-2799, CVE-2014-4059, CVE-2014-4065, CVE-2014-4079, CVE-2014-4081, CVE-2014-4083, CVE-2014-4085, CVE-2014-4088, CVE-2014-4090, CVE-2014-4094, CVE-2014-4100, CVE-2014-4103, CVE-2014-4104, CVE-2014-4105, CVE-2014-4106, CVE-2014-4107, CVE-2014-4108, CVE-2014-4109, CVE-2014-4110, and CVE-2014-4111.

CVE ID: CVE-2014-4100
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-2799, CVE-2014-4059, CVE-2014-4065, CVE-2014-4079, CVE-2014-4081, CVE-2014-4083, CVE-2014-4085, CVE-2014-4088, CVE-2014-4090, CVE-2014-4094, CVE-2014-4097, CVE-2014-4103, CVE-2014-4104, CVE-2014-4105, CVE-2014-4106, CVE-2014-4107, CVE-2014-4108, CVE-2014-4109, CVE-2014-4110, and CVE-2014-4111.

CVE ID: CVE-2014-4103
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-2799, CVE-2014-4059, CVE-2014-4065, CVE-2014-4079, CVE-2014-4081, CVE-2014-4083, CVE-2014-4085, CVE-2014-4088, CVE-2014-4090, CVE-2014-4094, CVE-2014-4097, CVE-2014-4100, CVE-2014-4104, CVE-2014-4105, CVE-2014-4106, CVE-2014-4107, CVE-2014-4108, CVE-2014-4109, CVE-2014-4110, and CVE-2014-4111.

CVE ID: CVE-2014-4104
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-2799, CVE-2014-4059, CVE-2014-4065, CVE-2014-4079, CVE-2014-4081, CVE-2014-4083, CVE-2014-4085, CVE-2014-4088, CVE-2014-4090, CVE-2014-4094, CVE-2014-4097, CVE-2014-4100, CVE-2014-4103, CVE-2014-4105, CVE-2014-4106, CVE-2014-4107, CVE-2014-4108, CVE-2014-4109, CVE-2014-4110, and CVE-2014-4111.

CVE ID: CVE-2014-4105
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-2799, CVE-2014-4059, CVE-2014-4065, CVE-2014-4079, CVE-2014-4081, CVE-2014-4083, CVE-2014-4085, CVE-2014-4088, CVE-2014-4090, CVE-2014-4094, CVE-2014-4097, CVE-2014-4100, CVE-2014-4103, CVE-2014-4104, CVE-2014-4106, CVE-2014-4107, CVE-2014-4108, CVE-2014-4109, CVE-2014-4110, and CVE-2014-4111.

CVE ID: CVE-2014-4106
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-2799, CVE-2014-4059, CVE-2014-4065, CVE-2014-4079, CVE-2014-4081, CVE-2014-4083, CVE-2014-4085, CVE-2014-4088, CVE-2014-4090, CVE-2014-4094, CVE-2014-4097, CVE-2014-4100, CVE-2014-4103, CVE-2014-4104, CVE-2014-4105, CVE-2014-4107, CVE-2014-4108, CVE-2014-4109, CVE-2014-4110, and CVE-2014-4111.

CVE ID: CVE-2014-4107
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-2799, CVE-2014-4059, CVE-2014-4065, CVE-2014-4079, CVE-2014-4081, CVE-2014-4083, CVE-2014-4085, CVE-2014-4088, CVE-2014-4090, CVE-2014-4094, CVE-2014-4097, CVE-2014-4100, CVE-2014-4103, CVE-2014-4104, CVE-2014-4105, CVE-20

14-4106, CVE-2014-4108, CVE-2014-4109, CVE-2014-4110, and CVE-2014-4111.

CVE ID: CVE-2014-4108
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-2799, CVE-2014-4059, CVE-2014-4065, CVE-2014-4079, CVE-2014-4081, CVE-2014-4083, CVE-2014-4085, CVE-2014-4088, CVE-2014-4090, CVE-2014-4094, CVE-2014-4097, CVE-2014-4100, CVE-2014-4103, CVE-2014-4104, CVE-2014-4105, CVE-2014-4106, CVE-2014-4107, CVE-2014-4109, CVE-2014-4110, and CVE-2014-4111.

CVE ID: CVE-2014-4109
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-2799, CVE-2014-4059, CVE-2014-4065, CVE-2014-4079, CVE-2014-4081, CVE-2014-4083, CVE-2014-4085, CVE-2014-4088, CVE-2014-4090, CVE-2014-4094, CVE-2014-4097, CVE-2014-4100, CVE-2014-4103, CVE-2014-4104, CVE-2014-4105, CVE-2014-4106, CVE-2014-4107, CVE-2014-4108, CVE-2014-4110, and CVE-2014-4111.

CVE ID: CVE-2014-4110
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-2799, CVE-2014-4059, CVE-2014-4065, CVE-2014-4079, CVE-2014-4081, CVE-2014-4083, CVE-2014-4085, CVE-2014-4088, CVE-2014-4090, CVE-2014-4094, CVE-2014-4097, CVE-2014-4100, CVE-2014-4103, CVE-2014-4104, CVE-2014-4105, CVE-2014-4106, CVE-2014-4107, CVE-2014-4108, CVE-2014-4109, and CVE-2014-4111.

CVE ID: CVE-2014-4111
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-2799, CVE-2014-4059, CVE-2014-4065, CVE-2014-4079, CVE-2014-4081, CVE-2014-4083, CVE-2014-4085, CVE-2014-4088, CVE-2014-4090, CVE-2014-4094, CVE-2014-4097, CVE-2014-4100, CVE-2014-4103, CVE-2014-4104, CVE-2014-4105, CVE-2014-4106, CVE-2014-4107, CVE-2014-4108, CVE-2014-4109, and CVE-2014-4110.

CVE ID: CVE-2014-4128
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability."

CVE ID: CVE-2014-4143
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-6341.

CVE ID: CVE-2014-6340
Severity: MODERATE
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to read content from a different (1) domain or (2) zone via a crafted web site, aka "Internet Explorer Cross-domain Information Disclosure Vulnerability."

CVE ID: CVE-2014-6341
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-4143.

CVE ID: CVE-2014-6363
Severity: CRITICAL
Description: vbscript.dll in Microsoft VBScript 5.6 through 5.8, as used with Internet Explorer 6 through 11 and other products, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "VBScript Memory Corruption Vulnerability."

CVE ID: CVE-2014-6374

Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability."

CVE ID: CVE-2015-0017
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-0020, CVE-2015-0022, CVE-2015-0026, CVE-2015 -0030, CVE-2015-0031, CVE-2015-0036, and CVE-2015-0041.

CVE ID: CVE-2015-0020
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-0017, CVE-2015-0022, CVE-2015-0026, CVE-2015 -0030, CVE-2015-0031, CVE-2015-0036, and CVE-2015-0041.

CVE ID: CVE-2015-0022
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-0017, CVE-2015-0020, CVE-2015-0026, CVE-2015 -0030, CVE-2015-0031, CVE-2015-0036, and CVE-2015-0041.

CVE ID: CVE-2015-0026
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-0017, CVE-2015-0020, CVE-2015-0022, CVE-2015 -0030, CVE-2015-0031, CVE-2015-0036, and CVE-2015-0041.

CVE ID: CVE-2015-0030
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-0017, CVE-2015-0020, CVE-2015-0022, CVE-2015 -0026, CVE-2015-0031, CVE-2015-0036, and CVE-2015-0041.

CVE ID: CVE-2015-0031
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-0017, CVE-2015-0020, CVE-2015-0022, CVE-2015 -0026, CVE-2015-0030, CVE-2015-0036, and CVE-2015-0041.

CVE ID: CVE-2015-0036
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-0017, CVE-2015-0020, CVE-2015-0022, CVE-2015 -0026, CVE-2015-0030, CVE-2015-0031, and CVE-2015-0041.

CVE ID: CVE-2015-0041
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-0017, CVE-2015-0020, CVE-2015-0022, CVE-2015 -0026, CVE-2015-0030, CVE-2015-0031, and CVE-2015-0036.

CVE ID: CVE-2015-0070
Severity: MODERATE
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to read content from a different (1) do main or (2) zone via a crafted web site, aka "Internet Explorer Cross-domain Information Disclosure Vul nerability."

CVE ID: CVE-2015-1625

Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-1634.

CVE ID: CVE-2015-1634
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-1625.

CVE ID: CVE-2015-1652
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-1666.

CVE ID: CVE-2015-1661
Severity: MODERATE
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to bypass the ASLR protection mecha nism via a crafted web site, aka "Internet Explorer ASLR Bypass Vulnerability."

CVE ID: CVE-2015-1666
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-1652.

CVE ID: CVE-2015-1694
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-1710.

CVE ID: CVE-2015-1703
Severity: IMPORTANT
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to gain privileges via a crafted web sit e, aka "Internet Explorer Elevation of Privilege Vulnerability," a different vulnerability than CVE-2015-17 04.

CVE ID: CVE-2015-1704
Severity: IMPORTANT
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to gain privileges via a crafted web sit e, aka "Internet Explorer Elevation of Privilege Vulnerability," a different vulnerability than CVE-2015-17 03.

CVE ID: CVE-2015-1710
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-1694.

CVE ID: CVE-2015-1735
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-1740, CVE-2015-1744, CVE-2015-1745, and CVE-2015-1766.

CVE ID: CVE-2015-1740
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-1735, CVE-2015-1744, CVE-2015-1745, and CVE-2015-1766.

CVE ID: CVE-2015-1744
Severity: CRITICAL

Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1735, CVE-2015-1740, CVE-2015-1745, and CVE-2015-1766.

CVE ID: CVE-2015-1745
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1735, CVE-2015-1740, CVE-2015-1744, and CVE-2015-1766.

CVE ID: CVE-2015-1766
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1735, CVE-2015-1740, CVE-2015-1744, and CVE-2015-1745.

CVE ID: CVE-2015-2385
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-2390, CVE-2015-2397, CVE-2015-2404, CVE-2015-2406, and CVE-2015-2422.

CVE ID: CVE-2015-2390
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-2385, CVE-2015-2397, CVE-2015-2404, CVE-2015-2406, and CVE-2015-2422.

CVE ID: CVE-2015-2397
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-2385, CVE-2015-2390, CVE-2015-2404, CVE-2015-2406, and CVE-2015-2422.

CVE ID: CVE-2015-2404
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-2385, CVE-2015-2390, CVE-2015-2397, CVE-2015-2406, and CVE-2015-2422.

CVE ID: CVE-2015-2406
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-2385, CVE-2015-2390, CVE-2015-2397, CVE-2015-2404, and CVE-2015-2422.

CVE ID: CVE-2015-2410
Severity: MODERATE
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to determine the existence of local files via a crafted stylesheet, aka "Internet Explorer Information Disclosure Vulnerability."

CVE ID: CVE-2015-2413
Severity: MODERATE
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to determine the existence of local files via a crafted module-resource request, aka "Internet Explorer Information Disclosure Vulnerability."

CVE ID: CVE-2015-2421
Severity: MODERATE
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to bypass the ASLR protection mechanism via a crafted web site, aka "Internet Explorer ASLR Bypass."

CVE ID: CVE-2015-2422
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-2385, CVE-2015-2390, CVE-2015-2397, CVE-2015-2404, and CVE-2015-2406.

CVE ID: CVE-2013-5046
Severity: IMPORTANT
Description: Microsoft Internet Explorer 7 through 11 allows local users to bypass the Protected Mode protection mechanism, and consequently gain privileges, by leveraging the ability to execute sandboxed code, aka "Internet Explorer Elevation of Privilege Vulnerability."

CVE ID: CVE-2014-1764
Severity: CRITICAL
Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to execute arbitrary code and bypass a sandbox protection mechanism by leveraging "object confusion" in a broker process, as demonstrated by VUPEN during a Pwn2Own competition at CanSecWest 2014.

CVE ID: CVE-2014-1791
Severity: CRITICAL
Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability."

CVE ID: CVE-2014-2783
Severity: IMPORTANT
Description: Microsoft Internet Explorer 7 through 11 does not prevent use of wildcard EV SSL certificates, which might allow remote attackers to spoof a trust level by leveraging improper issuance of a wildcard certificate by a recognized Certification Authority, aka "Extended Validation (EV) Certificate Security Feature Bypass Vulnerability."

CVE ID: CVE-2014-2819
Severity: IMPORTANT
Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to gain privileges via a crafted web site, aka "Internet Explorer Elevation of Privilege Vulnerability."

CVE ID: CVE-2014-4056
Severity: CRITICAL
Description: Microsoft Internet Explorer 7 through 10 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability."

CVE ID: CVE-2014-4123
Severity: IMPORTANT
Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to gain privileges via a crafted web site, aka "Internet Explorer Elevation of Privilege Vulnerability," as exploited in the wild in October 2014, a different vulnerability than CVE-2014-4124.

CVE ID: CVE-2014-4124
Severity: IMPORTANT
Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to gain privileges via a crafted web site, aka "Internet Explorer Elevation of Privilege Vulnerability," a different vulnerability than CVE-2014-4123.

CVE ID: CVE-2014-6323
Severity: MODERATE
Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to obtain sensitive clipboard information via a crafted web site, aka "Internet Explorer Clipboard Information Disclosure Vulnerability."

CVE ID: CVE-2015-1627
Severity: MODERATE
Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to gain privileges via a crafted web site, aka "Internet Explorer Elevation of Privilege Vulnerability."

CVE ID: CVE-2015-1688
Severity: IMPORTANT

Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to gain privileges via a crafted web sit e, aka "Internet Explorer Elevation of Privilege Vulnerability."

CVE ID: CVE-2015-1692
Severity: MODERATE
Description: Microsoft Internet Explorer 7 through 11 allows user-assisted remote attackers to read the clipboard co ntents via crafted web script, aka "Internet Explorer Clipboard Information Disclosure Vulnerability."

CVE ID: CVE-2015-1709
Severity: CRITICAL
Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability."

CVE ID: CVE-2015-1743
Severity: IMPORTANT
Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to gain privileges via a crafted web sit e, aka "Internet Explorer Elevation of Privilege Vulnerability," a different vulnerability than CVE-2015-17 48.

CVE ID: CVE-2015-1748
Severity: IMPORTANT
Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to gain privileges via a crafted web sit e, aka "Internet Explorer Elevation of Privilege Vulnerability," a different vulnerability than CVE-2015-17 43.

CVE ID: CVE-2015-2402
Severity: MODERATE
Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to gain privileges via a crafted web sit e, aka "Internet Explorer Elevation of Privilege Vulnerability."

CVE ID: CVE-2015-2423
Severity: MODERATE
Description: Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, W indows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, Windows 10, Excel 2007 S P3, PowerPoint 2007 SP3, Visio 2007 SP3, Word 2007 SP3, Office 2010 SP2, Excel 2010 SP2, Power Point 2010 SP2, Visio 2010 SP2, Word 2010 SP2, Excel 2013 SP1, PowerPoint 2013 SP1, Visio 2013 SP1, Word 2013 SP1, Excel 2013 RT SP1, PowerPoint 2013 RT SP1, Visio 2013 RT SP1, Word 2013 RT SP1, and Internet Explorer 7 through 11 allow remote attackers to gain privileges and obtain sensitiv e information via a crafted command-line parameter to an Office application or Notepad, as demonstrate d by a transition from Low Integrity to Medium Integrity, aka "Unsafe Command Line Parameter Passing Vulnerability."

CVE ID: CVE-2015-2441
Severity: CRITICAL
Description: Microsoft Internet Explorer 7 through 11 and Edge allow remote attackers to execute arbitrary code or c ause a denial of service (memory corruption) via a crafted web site, aka "Memory Corruption Vulnerabilit y," a different vulnerability than CVE-2015-2452.

CVE ID: CVE-2015-2449
Severity: MODERATE
Description: Microsoft Internet Explorer 7 through 11 and Edge allow remote attackers to bypass the ASLR protectio n mechanism via a crafted web site, aka "ASLR Bypass."

CVE ID: CVE-2015-2452
Severity: CRITICAL
Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Memory Corruption Vulnerability," a diff erent vulnerability than CVE-2015-2441.

CVE ID: CVE-2015-2486
Severity: CRITICAL
Description: Microsoft Internet Explorer 7 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Memory Corruption V ulnerability," a different vulnerability than CVE-2015-2487, CVE-2015-2490, CVE-2015-2492, CVE-2015 -2494, CVE-2015-2498, and CVE-2015-2499.

CVE ID: CVE-2015-2487

Severity: CRITICAL
Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Memory Corruption Vulnerability," a different vulnerability than CVE-2015-2486, CVE-2015-2490, CVE-2015-2492, CVE-2015-2494, CVE-2015-2498, and CVE-2015-2499.

CVE ID: CVE-2015-2490
Severity: CRITICAL
Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Memory Corruption Vulnerability," a different vulnerability than CVE-2015-2486, CVE-2015-2487, CVE-2015-2492, CVE-2015-2494, CVE-2015-2498, and CVE-2015-2499.

CVE ID: CVE-2015-2492
Severity: CRITICAL
Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Memory Corruption Vulnerability," a different vulnerability than CVE-2015-2486, CVE-2015-2487, CVE-2015-2490, CVE-2015-2494, CVE-2015-2498, and CVE-2015-2499.

CVE ID: CVE-2015-2494
Severity: CRITICAL
Description: Microsoft Internet Explorer 7 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Memory Corruption Vulnerability," a different vulnerability than CVE-2015-2486, CVE-2015-2487, CVE-2015-2490, CVE-2015-2492, CVE-2015-2498, and CVE-2015-2499.

CVE ID: CVE-2015-2498
Severity: CRITICAL
Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Memory Corruption Vulnerability," a different vulnerability than CVE-2015-2486, CVE-2015-2487, CVE-2015-2490, CVE-2015-2492, CVE-2015-2494, and CVE-2015-2499.

CVE ID: CVE-2015-2499
Severity: CRITICAL
Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Memory Corruption Vulnerability," a different vulnerability than CVE-2015-2486, CVE-2015-2487, CVE-2015-2490, CVE-2015-2492, CVE-2015-2494, and CVE-2015-2498.

CVE ID: CVE-2015-2502
Severity: CRITICAL
Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Memory Corruption Vulnerability," as exploited in the wild in August 2015.

CVE ID: CVE-2015-6048
Severity: CRITICAL
Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-6049.

CVE ID: CVE-2015-6049
Severity: CRITICAL
Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-6048.

CVE ID: CVE-2015-6066
Severity: CRITICAL
Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-6070, CVE-2015-6071, CVE-2015-6074, CVE-2015-6076, and CVE-2015-6087.

CVE ID: CVE-2015-6070
Severity: CRITICAL

Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-6066, CVE-2015-6071, CVE-2015-6074, CVE-2015 -6076, and CVE-2015-6087.

CVE ID: CVE-2015-6071
Severity: CRITICAL
Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-6066, CVE-2015-6070, CVE-2015-6074, CVE-2015 -6076, and CVE-2015-6087.

CVE ID: CVE-2015-6074
Severity: CRITICAL
Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-6066, CVE-2015-6070, CVE-2015-6071, CVE-2015 -6076, and CVE-2015-6087.

CVE ID: CVE-2015-6076
Severity: CRITICAL
Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-6066, CVE-2015-6070, CVE-2015-6071, CVE-2015 -6074, and CVE-2015-6087.

CVE ID: CVE-2015-6087
Severity: CRITICAL
Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-6066, CVE-2015-6070, CVE-2015-6071, CVE-2015 -6074, and CVE-2015-6076.

CVE ID: CVE-2015-6150
Severity: CRITICAL
Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-6154.

CVE ID: CVE-2015-6154
Severity: CRITICAL
Description: Microsoft Internet Explorer 7 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Me mory Corruption Vulnerability," a different vulnerability than CVE-2015-6150.

CVE ID: CVE-2015-6161
Severity: MODERATE
Description: Microsoft Internet Explorer 7 through 11 and Microsoft Edge allow remote attackers to bypass the ASL R protection mechanism via a crafted web site, aka "Microsoft Browser ASLR Bypass."

CVE ID: CVE-2015-6184
Severity: CRITICAL
Description: The CAttrArray object implementation in Microsoft Internet Explorer 7 through 11 allows remote attacke rs to execute arbitrary code or cause a denial of service (type confusion and memory corruption) via a m alformed Cascading Style Sheets (CSS) token sequence in conjunction with modifications to HTML ele ments, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-6048 and CVE-2015-6049.

CVE ID: CVE-2013-3912
Severity: CRITICAL
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2013-3916.

CVE ID: CVE-2013-3916
Severity: CRITICAL
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V

ulnerability," a different vulnerability than CVE-2013-3912.

CVE ID: CVE-2014-0268
Severity: MODERATE
Description: Microsoft Internet Explorer 8 through 11 does not properly restrict file installation and registry-key creati on, which allows remote attackers to bypass the Mandatory Integrity Control protection mechanism via a crafted web site, aka "Internet Explorer Elevation of Privilege Vulnerability."

CVE ID: CVE-2014-0281
Severity: CRITICAL
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-0287.

CVE ID: CVE-2014-0287
Severity: CRITICAL
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-0281.

CVE ID: CVE-2014-0297
Severity: CRITICAL
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-0308, CVE-2014-0312, and CVE-2014-0324.

CVE ID: CVE-2014-0308
Severity: CRITICAL
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-0297, CVE-2014-0312, and CVE-2014-0324.

CVE ID: CVE-2014-0312
Severity: CRITICAL
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-0297, CVE-2014-0308, and CVE-2014-0324.

CVE ID: CVE-2014-0324
Severity: CRITICAL
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-0297, CVE-2014-0308, and CVE-2014-0312.

CVE ID: CVE-2014-1778
Severity: IMPORTANT
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary web script with inc reased privileges via unspecified vectors, aka "Internet Explorer Elevation of Privilege Vulnerability," a di fferent vulnerability than CVE-2014-2777.

CVE ID: CVE-2014-1800
Severity: CRITICAL
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability."

CVE ID: CVE-2014-2777
Severity: IMPORTANT
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary web script with inc reased privileges via unspecified vectors, aka "Internet Explorer Elevation of Privilege Vulnerability," a di fferent vulnerability than CVE-2014-1778.

CVE ID: CVE-2014-2784
Severity: CRITICAL
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-4051.

CVE ID: CVE-2014-2789

Severity: CRITICAL
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-2795, CVE-2014-2798, and CVE-2014-2804.

CVE ID: CVE-2014-2795
Severity: CRITICAL
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-2789, CVE-2014-2798, and CVE-2014-2804.

CVE ID: CVE-2014-2798
Severity: CRITICAL
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-2789, CVE-2014-2795, and CVE-2014-2804.

CVE ID: CVE-2014-2804
Severity: CRITICAL
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-2789, CVE-2014-2795, and CVE-2014-2798.

CVE ID: CVE-2014-4051
Severity: CRITICAL
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-2784.

CVE ID: CVE-2014-4092
Severity: CRITICAL
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-4098.

CVE ID: CVE-2014-4098
Severity: CRITICAL
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-4092.

CVE ID: CVE-2014-4140
Severity: MODERATE
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to bypass the ASLR protection mecha nism via a crafted web site, aka "Internet Explorer ASLR Bypass Vulnerability."

CVE ID: CVE-2014-4141
Severity: CRITICAL
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability."

CVE ID: CVE-2014-6328
Severity: MODERATE
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to bypass the XSS filter via a crafted a ttribute of an element in an HTML document, aka "Internet Explorer XSS Filter Bypass Vulnerability," a d ifferent vulnerability than CVE-2014-6365.

CVE ID: CVE-2014-6346
Severity: MODERATE
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to read content from a different (1) do main or (2) zone via a crafted web site, aka "Internet Explorer Cross-domain Information Disclosure Vul nerability."

CVE ID: CVE-2014-6351
Severity: CRITICAL
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V

ulnerability."

CVE ID: CVE-2014-6365
Severity: MODERATE
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to bypass the XSS filter via a crafted a ttribute of an element in an HTML document, aka "Internet Explorer XSS Filter Bypass Vulnerability," a d ifferent vulnerability than CVE-2014-6328.

CVE ID: CVE-2015-0032
Severity: CRITICAL
Description: vbscript.dll in Microsoft VBScript 5.6 through 5.8, as used with Internet Explorer 8 through 11 and other products, allows remote attackers to execute arbitrary code or cause a denial of service (memory corrup tion) via a crafted web site, aka "VBScript Memory Corruption Vulnerability."

CVE ID: CVE-2015-0043
Severity: CRITICAL
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability."

CVE ID: CVE-2015-1624
Severity: CRITICAL
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability."

CVE ID: CVE-2015-1667
Severity: CRITICAL
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability."

CVE ID: CVE-2015-1684
Severity: MODERATE
Description: VBScript.dll in the Microsoft VBScript 5.6 through 5.8 engine, as used in Internet Explorer 8 through 11 and other products, allows remote attackers to bypass the ASLR protection mechanism via a crafted we b site, aka "VBScript ASLR Bypass."

CVE ID: CVE-2015-1686
Severity: MODERATE
Description: The Microsoft (1) VBScript 5.6 through 5.8 and (2) JScript 5.6 through 5.8 engines, as used in Internet Explorer 8 through 11 and other products, allow remote attackers to bypass the ASLR protection mecha nism via a crafted web site, aka "VBScript and JScript ASLR Bypass."

CVE ID: CVE-2015-2398
Severity: MODERATE
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to bypass the XSS filter via a crafted a ttribute of an element in an HTML document, aka "Internet Explorer XSS Filter Bypass Vulnerability."

CVE ID: CVE-2015-2414
Severity: MODERATE
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to obtain sensitive browsing-history inf ormation via vectors related to image caching, aka "Internet Explorer Information Disclosure Vulnerabilit y."

CVE ID: CVE-2015-2442
Severity: CRITICAL
Description: Microsoft Internet Explorer 8 through 11 and Edge allow remote attackers to execute arbitrary code or c ause a denial of service (memory corruption) via a crafted web site, aka "Memory Corruption Vulnerabilit y," a different vulnerability than CVE-2015-2444.

CVE ID: CVE-2015-2444
Severity: CRITICAL
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Memory Corruption Vulnerability," a diff erent vulnerability than CVE-2015-2442.

CVE ID: CVE-2015-6047

Severity: IMPORTANT
Description: The broker EditWith feature in Microsoft Internet Explorer 8 through 11 allows remote attackers to bypass the AppContainer protection mechanism and gain privileges via a DelegateExecute launch of an arbitrary application, as demonstrated by a transition from Low Integrity to Medium Integrity, aka "Internet Explorer Elevation of Privilege Vulnerability."

CVE ID: CVE-2015-6052
Severity: MODERATE
Description: The Microsoft (1) VBScript 5.7 and 5.8 and (2) JScript 5.7 and 5.8 engines, as used in Internet Explorer 8 through 11 and other products, allow remote attackers to bypass the ASLR protection mechanism via a crafted web site, aka "VBScript and JScript ASLR Bypass."

CVE ID: CVE-2015-6059
Severity: MODERATE
Description: The Microsoft (1) VBScript 5.7 and 5.8 and (2) JScript 5.7 and 5.8 engines, as used in Internet Explorer 8 through 11 and other products, allow remote attackers to obtain sensitive information from process memory via a crafted web site, aka "Scripting Engine Information Disclosure Vulnerability."

CVE ID: CVE-2015-6069
Severity: CRITICAL
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-6081.

CVE ID: CVE-2015-6081
Severity: CRITICAL
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-6069.

CVE ID: CVE-2015-6083
Severity: CRITICAL
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-6151.

CVE ID: CVE-2015-6138
Severity: MODERATE
Description: Microsoft Internet Explorer 8 through 11 mishandles HTML attributes in HTTP responses, which allows remote attackers to bypass a cross-site scripting (XSS) protection mechanism via unspecified vectors, aka "Internet Explorer XSS Filter Bypass Vulnerability."

CVE ID: CVE-2015-6144
Severity: MODERATE
Description: Microsoft Internet Explorer 8 through 11 and Microsoft Edge mishandle HTML attributes in HTTP responses, which allows remote attackers to bypass a cross-site scripting (XSS) protection mechanism via unspecified vectors, aka "Microsoft Browser XSS Filter Bypass Vulnerability."

CVE ID: CVE-2015-6151
Severity: CRITICAL
Description: Microsoft Internet Explorer 8 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability," a different vulnerability than CVE-2015-6083.

CVE ID: CVE-2013-3914
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability."

CVE ID: CVE-2014-0270
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-0273, CVE-2014-0274, and CVE-2014-0288.

CVE ID: CVE-2014-0273
Severity: CRITICAL

Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-0270, CVE-2014-0274, and CVE-2014-0288.

CVE ID: CVE-2014-0274
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-0270, CVE-2014-0273, and CVE-2014-0288.

CVE ID: CVE-2014-0288
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-0270, CVE-2014-0273, and CVE-2014-0274.

CVE ID: CVE-2014-0293
Severity: MODERATE
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to read content from a different (1) do main or (2) zone via a crafted web site, aka "Internet Explorer Cross-domain Information Disclosure Vul nerability."

CVE ID: CVE-2014-0298
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability."

CVE ID: CVE-2014-1763
Severity: CRITICAL
Description: Use-after-free vulnerability in Microsoft Internet Explorer 9 through 11 allows remote attackers to execut e arbitrary code and bypass a sandbox protection mechanism via unspecified vectors, as demonstrated by VUPEN during a Pwn2Own competition at CanSecWest 2014.

CVE ID: CVE-2014-1773
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-1783, CVE-2014-1784, CVE-2014-1786, CVE-2014 -1795, CVE-2014-1805, CVE-2014-2758, CVE-2014-2759, CVE-2014-2765, CVE-2014-2766, and CVE-

CVE ID: CVE-2014-1783
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-1773, CVE-2014-1784, CVE-2014-1786, CVE-2014 -1795, CVE-2014-1805, CVE-2014-2758, CVE-2014-2759, CVE-2014-2765, CVE-2014-2766, and CVE-

CVE ID: CVE-2014-1784
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-1773, CVE-2014-1783, CVE-2014-1786, CVE-2014 -1795, CVE-2014-1805, CVE-2014-2758, CVE-2014-2759, CVE-2014-2765, CVE-2014-2766, and CVE-

CVE ID: CVE-2014-1786
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-1773, CVE-2014-1783, CVE-2014-1784, CVE-2014 -1795, CVE-2014-1805, CVE-2014-2758, CVE-2014-2759, CVE-2014-2765, CVE-2014-2766, and CVE-

CVE ID: CVE-2014-1795
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-1773, CVE-2014-1783, CVE-2014-1784, CVE-2014 -1786, CVE-2014-1805, CVE-2014-2758, CVE-2014-2759, CVE-2014-2765, CVE-2014-2766, and CVE-

CVE ID: CVE-2014-1805
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-1773, CVE-2014-1783, CVE-2014-1784, CVE-2014 -1786, CVE-2014-1795, CVE-2014-2758, CVE-2014-2759, CVE-2014-2765, CVE-2014-2766, and CVE-

CVE ID: CVE-2014-2758
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-1773, CVE-2014-1783, CVE-2014-1784, CVE-2014 -1786, CVE-2014-1795, CVE-2014-1805, CVE-2014-2759, CVE-2014-2765, CVE-2014-2766, and CVE-

CVE ID: CVE-2014-2759
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-1773, CVE-2014-1783, CVE-2014-1784, CVE-2014 -1786, CVE-2014-1795, CVE-2014-1805, CVE-2014-2758, CVE-2014-2765, CVE-2014-2766, and CVE-

CVE ID: CVE-2014-2765
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-1773, CVE-2014-1783, CVE-2014-1784, CVE-2014 -1786, CVE-2014-1795, CVE-2014-1805, CVE-2014-2758, CVE-2014-2759, CVE-2014-2766, and CVE-

CVE ID: CVE-2014-2766
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-1773, CVE-2014-1783, CVE-2014-1784, CVE-2014 -1786, CVE-2014-1795, CVE-2014-1805, CVE-2014-2758, CVE-2014-2759, CVE-2014-2765, and CVE-

CVE ID: CVE-2014-2775
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-1773, CVE-2014-1783, CVE-2014-1784, CVE-2014 -1786, CVE-2014-1795, CVE-2014-1805, CVE-2014-2758, CVE-2014-2759, CVE-2014-2765, and CVE-

CVE ID: CVE-2014-2782
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-1773, CVE-2014-1783, CVE-2014-1784, CVE-2014 -1786, CVE-2014-1795, CVE-2014-1805, CVE-2014-2758, CVE-2014-2759, CVE-2014-2765, CVE-201 4-2766, and CVE-2014-2775.

CVE ID: CVE-2014-2786
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-2792 and CVE-2014-2813.

CVE ID: CVE-2014-2792
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-2786 and CVE-2014-2813.

CVE ID: CVE-2014-2813
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-2786 and CVE-2014-2792.

CVE ID: CVE-2014-4058
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability."

CVE ID: CVE-2014-4099
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability."

CVE ID: CVE-2014-6343
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability."

CVE ID: CVE-2014-6369
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability."

CVE ID: CVE-2015-0038
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-0042 and CVE-2015-0046.

CVE ID: CVE-2015-0042
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-0038 and CVE-2015-0046.

CVE ID: CVE-2015-0046
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-0038 and CVE-2015-0042.

CVE ID: CVE-2015-0071
Severity: MODERATE
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to bypass the ASLR protection mecha nism via a crafted web site, aka "Internet Explorer ASLR Bypass Vulnerability."

CVE ID: CVE-2015-0072
Severity: MODERATE
Description: Cross-site scripting (XSS) vulnerability in Microsoft Internet Explorer 9 through 11 allows remote attack ers to bypass the Same Origin Policy and inject arbitrary web script or HTML via vectors involving an IF RAME element that triggers a redirect, a second IFRAME element that does not trigger a redirect, and a n eval of a WindowProxy object, aka "Universal XSS (UXSS)."

CVE ID: CVE-2015-1657
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability."

CVE ID: CVE-2015-1689
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-1705.

CVE ID: CVE-2015-1705

Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-1689.

CVE ID: CVE-2015-1729
Severity: MODERATE
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to read content from a different (1) do main or (2) zone via a crafted web site, aka "Internet Explorer Information Disclosure Vulnerability."

CVE ID: CVE-2015-1741
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-1752.

CVE ID: CVE-2015-1752
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-1741.

CVE ID: CVE-2015-1765
Severity: MODERATE
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to read the browser history via a crafte d web site.

CVE ID: CVE-2015-1767
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-2401 and CVE-2015-2408.

CVE ID: CVE-2015-2401
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-1767 and CVE-2015-2408.

CVE ID: CVE-2015-2408
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-1767 and CVE-2015-2401.

CVE ID: CVE-2015-2450
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Memory Corruption Vulnerability," a diff erent vulnerability than CVE-2015-2451.

CVE ID: CVE-2015-2451
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Memory Corruption Vulnerability," a diff erent vulnerability than CVE-2015-2450.

CVE ID: CVE-2015-2485
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Memory Corruption V ulnerability," a different vulnerability than CVE-2015-2491 and CVE-2015-2541.

CVE ID: CVE-2015-2491
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Memory Corruption Vulnerability," a diff erent vulnerability than CVE-2015-2485 and CVE-2015-2541.

CVE ID: CVE-2015-2541
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Memory Corruption Vulnerability," a diff erent vulnerability than CVE-2015-2485 and CVE-2015-2491.

CVE ID: CVE-2015-6046
Severity: MODERATE
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to obtain sensitive information from pr ocess memory via a crafted web site, aka "Internet Explorer Information Disclosure Vulnerability."

CVE ID: CVE-2015-6065
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-6078.

CVE ID: CVE-2015-6078
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Me mory Corruption Vulnerability," a different vulnerability than CVE-2015-6065.

CVE ID: CVE-2015-6086
Severity: MODERATE
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to obtain sensitive information from pr ocess memory via a crafted web site, aka "Internet Explorer Information Disclosure Vulnerability."

CVE ID: CVE-2015-6088
Severity: MODERATE
Description: Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to bypass the ASL R protection mechanism via a crafted web site, aka "Microsoft Browser ASLR Bypass."

CVE ID: CVE-2015-6148
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Me mory Corruption Vulnerability," a different vulnerability than CVE-2015-6156.

CVE ID: CVE-2015-6156
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-6148.

CVE ID: CVE-2015-6164
Severity: IMPORTANT
Description: Microsoft Internet Explorer 9 through 11 improperly implements a cross-site scripting (XSS) protection mechanism, which allows remote attackers to bypass the Same Origin Policy via a crafted web site, aka "Internet Explorer XSS Filter Bypass Vulnerability."

CVE ID: CVE-2016-0005
Severity: MODERATE
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to bypass the Same Origin Policy via u nspecified vectors, aka "Internet Explorer Elevation of Privilege Vulnerability."

CVE ID: CVE-2016-0059
Severity: MODERATE
Description: The Hyperlink Object Library in Microsoft Internet Explorer 9 through 11 allows remote attackers to obta in sensitive information from process memory via a crafted URL in a (1) e-mail message or (2) Office do cument, aka "Internet Explorer Information Disclosure Vulnerability."

CVE ID: CVE-2016-0060
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Me mory Corruption Vulnerability," a different vulnerability than CVE-2016-0061, CVE-2016-0063, CVE-201

6-0067, and CVE-2016-0072.

CVE ID: CVE-2016-0061
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0060, CVE-2016-0063, CVE-2016-0067, and CVE-2016-0072.

CVE ID: CVE-2016-0063
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0060, CVE-2016-0061, CVE-2016-0067, and CVE-2016-0072.

CVE ID: CVE-2016-0067
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0060, CVE-2016-0061, CVE-2016-0063, and CVE-2016-0072.

CVE ID: CVE-2016-0068
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to bypass the Same Origin Policy via unspecified vectors, aka "Internet Explorer Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-0069.

CVE ID: CVE-2016-0069
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to bypass the Same Origin Policy via unspecified vectors, aka "Internet Explorer Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-0068.

CVE ID: CVE-2016-0072
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0060, CVE-2016-0061, CVE-2016-0063, and CVE-2016-0067.

CVE ID: CVE-2016-0077
Severity: MODERATE
Description: Microsoft Internet Explorer 9 through 11 and Microsoft Edge misparse HTTP responses, which allows remote attackers to spoof web sites via a crafted URL, aka "Microsoft Browser Spoofing Vulnerability."

CVE ID: CVE-2016-0105
Severity: IMPORTANT
Description: Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0107, CVE-2016-0111, CVE-2016-0112, and CVE-2016-0113.

CVE ID: CVE-2016-0107
Severity: IMPORTANT
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0105, CVE-2016-0111, CVE-2016-0112, and CVE-2016-0113.

CVE ID: CVE-2016-0111
Severity: IMPORTANT
Description: Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0105, CVE-2016-0107, CVE-2016-0112, and CVE-2016-0113.

CVE ID: CVE-2016-0112
Severity: IMPORTANT
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2016-0105, CVE-2016-0107, CVE-2016-0111, and CVE-2016-0113.

CVE ID: CVE-2016-0113
Severity: IMPORTANT
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2016-0105, CVE-2016-0107, CVE-2016-0111, and CVE-2016-0112.

CVE ID: CVE-2016-0154
Severity: IMPORTANT
Description: Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Me mory Corruption Vulnerability."

CVE ID: CVE-2016-0162
Severity: MODERATE
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to determine the existence of files via crafted JavaScript code, aka "Internet Explorer Information Disclosure Vulnerability."

CVE ID: CVE-2016-0192
Severity: IMPORTANT
Description: Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Me mory Corruption Vulnerability."

CVE ID: CVE-2016-0199
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2016-0200 and CVE-2016-3211.

CVE ID: CVE-2016-0200
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2016-0199 and CVE-2016-3211.

CVE ID: CVE-2016-3204
Severity: CRITICAL
Description: The Microsoft (1) JScript 5.8 and 9 and (2) VBScript 5.7 and 5.8 engines, as used in Internet Explorer 9 through 11 and other products, allow remote attackers to execute arbitrary code or cause a denial of ser vice (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability."

CVE ID: CVE-2016-3211
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2016-0199 and CVE-2016-0200.

CVE ID: CVE-2016-3212
Severity: MODERATE
Description: The XSS Filter in Microsoft Internet Explorer 9 through 11 does not properly identify JavaScript, which makes it easier for remote attackers to conduct cross-site scripting (XSS) attacks via a crafted web site, aka "Internet Explorer XSS Filter Vulnerability."

CVE ID: CVE-2016-3213
Severity: CRITICAL
Description: The Web Proxy Auto Discovery (WPAD) protocol implementation in Microsoft Windows Vista SP2, Win dows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2 , Windows RT 8.1, Windows 10 Gold and 1511, and Internet Explorer 9 through 11 has an improper fall back mechanism, which allows remote attackers to gain privileges via NetBIOS name responses, aka "

WPAD Elevation of Privilege Vulnerability."

CVE ID: CVE-2016-3240
Severity: IMPORTANT
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2016-3241 and CVE-2016-3242.

CVE ID: CVE-2016-3241
Severity: IMPORTANT
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2016-3240 and CVE-2016-3242.

CVE ID: CVE-2016-3242
Severity: IMPORTANT
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2016-3240 and CVE-2016-3241.

CVE ID: CVE-2016-3245
Severity: MODERATE
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to trick users into making TCP connect ions to a restricted port via a crafted web site, aka "Internet Explorer Security Feature Bypass Vulnerabil ity."

CVE ID: CVE-2016-3248
Severity: CRITICAL
Description: The Microsoft (1) JScript 9, (2) VBScript, and (3) Chakra JavaScript engines, as used in Microsoft Inter net Explorer 9 through 11, Microsoft Edge, and other products, allow remote attackers to execute arbitra ry code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine M emory Corruption Vulnerability," a different vulnerability than CVE-2016-3259.

CVE ID: CVE-2016-3259
Severity: CRITICAL
Description: The Microsoft (1) JScript 9, (2) VBScript, and (3) Chakra JavaScript engines, as used in Microsoft Inter net Explorer 9 through 11, Microsoft Edge, and other products, allow remote attackers to execute arbitra ry code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine M emory Corruption Vulnerability," a different vulnerability than CVE-2016-3248.

CVE ID: CVE-2016-3264
Severity: IMPORTANT
Description: Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Me mory Corruption Vulnerability."

CVE ID: CVE-2016-3267
Severity: MODERATE
Description: Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to determine the ex istence of unspecified files via a crafted web site, aka "Microsoft Browser Information Disclosure Vulnera bility."

CVE ID: CVE-2016-3273
Severity: LOW
Description: The XSS Filter in Microsoft Internet Explorer 9 through 11 and Microsoft Edge does not properly restrict JavaScript code, which allows remote attackers to obtain sensitive information via a crafted web site, ak a "Microsoft Browser Information Disclosure Vulnerability."

CVE ID: CVE-2016-3274
Severity: LOW
Description: Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to conduct content-spoofing attacks via a crafted URL, aka "Microsoft Browser Spoofing Vulnerability."

CVE ID: CVE-2016-3293
Severity: IMPORTANT
Description: Microsoft Internet Explorer 9 through 11 and Edge allow remote attackers to execute arbitrary code via a crafted web page, aka "Microsoft Browser Memory Corruption Vulnerability."

CVE ID: CVE-2016-3297

Severity: IMPORTANT
Description: Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability."

CVE ID: CVE-2016-3298
Severity: LOW
Description: Microsoft Internet Explorer 9 through 11 and the Internet Messaging API in Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allow remote attackers to determine the existence of arbitrary files via a crafted web site, aka "Internet Explorer Information Disclosure Vulnerability."

CVE ID: CVE-2016-3324
Severity: IMPORTANT
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability."

CVE ID: CVE-2016-3326
Severity: LOW
Description: Microsoft Internet Explorer 9 through 11 and Edge allow remote attackers to obtain sensitive information via a crafted web page, aka "Microsoft Browser Information Disclosure Vulnerability," a different vulnerability than CVE-2016-3327.

CVE ID: CVE-2016-3327
Severity: LOW
Description: Microsoft Internet Explorer 9 through 11 and Edge allow remote attackers to obtain sensitive information via a crafted web page, aka "Microsoft Browser Information Disclosure Vulnerability," a different vulnerability than CVE-2016-3326.

CVE ID: CVE-2016-3329
Severity: LOW
Description: Microsoft Internet Explorer 9 through 11 and Edge allow remote attackers to determine the existence of files via a crafted webpage, aka "Internet Explorer Information Disclosure Vulnerability."

CVE ID: CVE-2016-3351
Severity: LOW
Description: Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to obtain sensitive information via a crafted web site, aka "Microsoft Browser Information Disclosure Vulnerability."

CVE ID: CVE-2016-3353
Severity: MODERATE
Description: Microsoft Internet Explorer 9 through 11 mishandles .url files from the Internet zone, which allows remote attackers to bypass intended access restrictions via a crafted file, aka "Internet Explorer Security Feature Bypass."

CVE ID: CVE-2016-3375
Severity: IMPORTANT
Description: The OLE Automation mechanism and VBScript scripting engine in Microsoft Internet Explorer 9 through 11, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability."

CVE ID: CVE-2016-3382
Severity: CRITICAL
Description: The scripting engines in Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, as demonstrated by the Chakra JavaScript engine, aka "Scripting Engine Memory Corruption Vulnerabilit

CVE ID: CVE-2016-3384
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability."

CVE ID: CVE-2016-3385
Severity: CRITICAL

Description: The scripting engine in Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbi trary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability."

CVE ID: CVE-2016-7195
Severity: IMPORTANT
Description: Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Me mory Corruption Vulnerability," a different vulnerability than CVE-2016-7198.

CVE ID: CVE-2016-7198
Severity: IMPORTANT
Description: Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Me mory Corruption Vulnerability," a different vulnerability than CVE-2016-7195.

CVE ID: CVE-2016-7199
Severity: LOW
Description: Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to bypass the Sam e Origin Policy and obtain sensitive window-state information via a crafted web site, aka "Microsoft Brow ser Information Disclosure Vulnerability."

CVE ID: CVE-2016-7227
Severity: LOW
Description: The scripting engines in Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attac kers to determine the existence of local files via unspecified vectors, aka "Microsoft Browser Information Disclosure Vulnerability."

CVE ID: CVE-2016-7239
Severity: LOW
Description: The RegEx class in the XSS filter in Microsoft Internet Explorer 9 through 11 and Microsoft Edge allows remote attackers to conduct cross-site scripting (XSS) attacks and obtain sensitive information via unsp ecified vectors, aka "Microsoft Browser Information Disclosure Vulnerability."

CVE ID: CVE-2016-7278
Severity: LOW
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to obtain sensitive information from pr ocess memory via a crafted web site, aka "Windows Hyperlink Object Library Information Disclosure Vul nerability."

CVE ID: CVE-2016-7279
Severity: IMPORTANT
Description: Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Me mory Corruption Vulnerability."

CVE ID: CVE-2016-7282
Severity: MODERATE
Description: Cross-site scripting (XSS) vulnerability in Microsoft Internet Explorer 9 through 11 and Microsoft Edge a llows remote attackers to inject arbitrary web script or HTML via unspecified vectors, aka "Microsoft Bro wser Information Disclosure Vulnerability."

CVE ID: CVE-2016-7283
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability."

CVE ID: CVE-2013-5045
Severity: IMPORTANT
Description: Microsoft Internet Explorer 10 and 11 allows local users to bypass the Protected Mode protection mech anism, and consequently gain privileges, by leveraging the ability to execute sandboxed code, aka "Inter net Explorer Elevation of Privilege Vulnerability."

CVE ID: CVE-2013-5051
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a deni al of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vuln

erability."

CVE ID: CVE-2014-0313
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-0321.

CVE ID: CVE-2014-0321
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-0313.

CVE ID: CVE-2014-1777
Severity: MODERATE
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to read local files on the client via a crafted web site, aka "Internet Explorer Information Disclosure Vulnerability."

CVE ID: CVE-2014-1780
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-1772, CVE-2014-1794, CVE-2014-1797, CVE-2014-1802, CVE-2014-2756, CVE-2014-2763, CVE-2014-2764, CVE-2014-2769, and CVE-2014-2771.

CVE ID: CVE-2014-1794
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-1772, CVE-2014-1780, CVE-2014-1797, CVE-2014-1802, CVE-2014-2756, CVE-2014-2763, CVE-2014-2764, CVE-2014-2769, and CVE-2014-2771.

CVE ID: CVE-2014-1797
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-1772, CVE-2014-1780, CVE-2014-1794, CVE-2014-1802, CVE-2014-2756, CVE-2014-2763, CVE-2014-2764, CVE-2014-2769, and CVE-2014-2771.

CVE ID: CVE-2014-1802
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-1772, CVE-2014-1780, CVE-2014-1794, CVE-2014-1797, CVE-2014-2756, CVE-2014-2763, CVE-2014-2764, CVE-2014-2769, and CVE-2014-2771.

CVE ID: CVE-2014-2756
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-1772, CVE-2014-1780, CVE-2014-1794, CVE-2014-1797, CVE-2014-1802, CVE-2014-2763, CVE-2014-2764, CVE-2014-2769, and CVE-2014-2771.

CVE ID: CVE-2014-2763
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-1772, CVE-2014-1780, CVE-2014-1794, CVE-2014-1797, CVE-2014-1802, CVE-2014-2756, CVE-2014-2764, CVE-2014-2769, and CVE-2014-2771.

CVE ID: CVE-2014-2764
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-1772, CVE-2014-1780, CVE-2014-1794, CVE-2014-1797, CVE-2014-1802, CVE-2014-2756, CVE-2014-2763, CVE-2014-2769, and CVE-2014-2771.

CVE ID: CVE-2014-2769

Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-1772, CVE-2014-1780, CVE-2014-1794, CVE-2014-1797, CVE-2014-1802, CVE-2014-2756, CVE-2014-2763, CVE-2014-2764, and CVE-2014-2771.

CVE ID: CVE-2014-2771
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-1772, CVE-2014-1780, CVE-2014-1794, CVE-2014-1797, CVE-2014-1802, CVE-2014-2756, CVE-2014-2763, CVE-2014-2764, and CVE-2014-2769.

CVE ID: CVE-2014-2796
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-2808, CVE-2014-2825, CVE-2014-4050, CVE-2014-4055, and CVE-2014-4067.

CVE ID: CVE-2014-2801
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability."

CVE ID: CVE-2014-2808
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-2796, CVE-2014-2825, CVE-2014-4050, CVE-2014-4055, and CVE-2014-4067.

CVE ID: CVE-2014-2825
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-2796, CVE-2014-2808, CVE-2014-4050, CVE-2014-4055, and CVE-2014-4067.

CVE ID: CVE-2014-4050
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-2796, CVE-2014-2808, CVE-2014-2825, CVE-2014-4055, and CVE-2014-4067.

CVE ID: CVE-2014-4055
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-2796, CVE-2014-2808, CVE-2014-2825, CVE-2014-4050, and CVE-2014-4067.

CVE ID: CVE-2014-4067
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-2796, CVE-2014-2808, CVE-2014-2825, CVE-2014-4050, and CVE-2014-4055.

CVE ID: CVE-2014-4080
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-4089, CVE-2014-4091, and CVE-2014-4102.

CVE ID: CVE-2014-4089

Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-4080, CVE-2014-4091, and CVE-2014-4102.

CVE ID: CVE-2014-4091
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-4080, CVE-2014-4089, and CVE-2014-4102.

CVE ID: CVE-2014-4102
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-4080, CVE-2014-4089, and CVE-2014-4091.

CVE ID: CVE-2014-4126
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability."

CVE ID: CVE-2014-6337
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability."

CVE ID: CVE-2014-6349
Severity: MODERATE
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to gain privileges via a crafted web site, aka "Internet Explorer Elevation of Privilege Vulnerability," a different vulnerability than CVE-2014-6350.

CVE ID: CVE-2014-6350
Severity: MODERATE
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to gain privileges via a crafted web site, aka "Internet Explorer Elevation of Privilege Vulnerability," a different vulnerability than CVE-2014-6349.

CVE ID: CVE-2015-0027
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-0035, CVE-2015-0039, CVE-2015-0052, and CVE-2015-0068.

CVE ID: CVE-2015-0035
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-0027, CVE-2015-0039, CVE-2015-0052, and CVE-2015-0068.

CVE ID: CVE-2015-0039
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-0027, CVE-2015-0035, CVE-2015-0052, and CVE-2015-0068.

CVE ID: CVE-2015-0052
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-0027, CVE-2015-0035, CVE-2015-0039, and CVE-2015-0068.

CVE ID: CVE-2015-0054

Severity: MODERATE
Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to gain privileges via a crafted web sit e, aka "Internet Explorer Elevation of Privilege Vulnerability."

CVE ID: CVE-2015-0055
Severity: MODERATE
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to gain privileges via a crafted web site, a ka "Internet Explorer Elevation of Privilege Vulnerability."

CVE ID: CVE-2015-0068
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a deni al of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vuln erability," a different vulnerability than CVE-2015-0027, CVE-2015-0035, CVE-2015-0039, and CVE-201 5-0052.

CVE ID: CVE-2015-0069
Severity: MODERATE
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to bypass the ASLR protection mechanis m via a crafted web site, aka "Internet Explorer ASLR Bypass Vulnerability."

CVE ID: CVE-2015-1622
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a deni al of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vuln erability."

CVE ID: CVE-2015-1668
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a deni al of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vuln erability."

CVE ID: CVE-2015-1714
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a deni al of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vuln erability."

CVE ID: CVE-2015-1731
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a deni al of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vuln erability," a different vulnerability than CVE-2015-1736, CVE-2015-1737, and CVE-2015-1755.

CVE ID: CVE-2015-1733
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a deni al of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vuln erability," a different vulnerability than CVE-2015-2389 and CVE-2015-2411.

CVE ID: CVE-2015-1736
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a deni al of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vuln erability," a different vulnerability than CVE-2015-1731, CVE-2015-1737, and CVE-2015-1755.

CVE ID: CVE-2015-1737
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a deni al of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vuln erability," a different vulnerability than CVE-2015-1731, CVE-2015-1736, and CVE-2015-1755.

CVE ID: CVE-2015-1739
Severity: IMPORTANT
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to gain privileges via a crafted web site, a ka "Internet Explorer Elevation of Privilege Vulnerability."

CVE ID: CVE-2015-1755

Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1731, CVE-2015-1736, and CVE-2015-1737.

CVE ID: CVE-2015-2389
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1733 and CVE-2015-2411.

CVE ID: CVE-2015-2411
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1733 and CVE-2015-2389.

CVE ID: CVE-2015-2412
Severity: MODERATE
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to read arbitrary local files via a crafted pathname, aka "Internet Explorer Information Disclosure Vulnerability."

CVE ID: CVE-2015-2419
Severity: CRITICAL
Description: JScript 9 in Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "JScript9 Memory Corruption Vulnerability."

CVE ID: CVE-2015-2443
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Memory Corruption Vulnerability."

CVE ID: CVE-2015-2483
Severity: MODERATE
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka "Information Disclosure Vulnerability."

CVE ID: CVE-2015-2484
Severity: IMPORTANT
Description: Microsoft Internet Explorer 10 and 11 uses an incorrect flag during certain filesystem accesses, which allows remote attackers to delete arbitrary files via unspecified vectors, aka "Tampering Vulnerability."

CVE ID: CVE-2015-2542
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Memory Corruption Vulnerability."

CVE ID: CVE-2015-6051
Severity: MODERATE
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to gain privileges via a crafted web site, as demonstrated by a transition from Low Integrity to Medium Integrity, aka "Internet Explorer Elevation of Privilege Vulnerability."

CVE ID: CVE-2015-6064
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability," a different vulnerability than CVE-2015-6084 and CVE-2015-6085.

CVE ID: CVE-2015-6084
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-6064 and CVE-2015-6085.

CVE ID: CVE-2015-6085

Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-6064 and CVE-2015-6084.

CVE ID: CVE-2015-6155
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability."

CVE ID: CVE-2016-0041
Severity: IMPORTANT
Description: Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold and 1511, and Internet Explorer 10 and 11 mishandle DLL loading, which allows local users to gain privileges via a crafted application, aka "DLL Loading Remote Code Execution Vulnerability."

CVE ID: CVE-2016-0110
Severity: IMPORTANT
Description: Microsoft Internet Explorer 10 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability."

CVE ID: CVE-2016-0164
Severity: IMPORTANT
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability."

CVE ID: CVE-2016-0194
Severity: LOW
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to bypass file permissions and obtain sensitive information via a crafted web site, aka "Internet Explorer Information Disclosure Vulnerability."

CVE ID: CVE-2016-1096
Severity: IMPORTANT
Description: Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.

CVE ID: CVE-2016-1097
Severity: IMPORTANT
Description: Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.

CVE ID: CVE-2016-1098
Severity: IMPORTANT
Description: Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.

CVE ID: CVE-2016-1099
Severity: IMPORTANT
Description: Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.

CVE ID: CVE-2016-1100
Severity: IMPORTANT
Description: Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.

CVE ID: CVE-2016-1101
Severity: IMPORTANT
Description: Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libra

ries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vector s, a different vulnerability than other CVEs listed in MS16-064.

CVE ID: CVE-2016-1102
Severity: IMPORTANT
Description: Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libra ries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vector s, a different vulnerability than other CVEs listed in MS16-064.

CVE ID: CVE-2016-1103
Severity: IMPORTANT
Description: Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libra ries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vector s, a different vulnerability than other CVEs listed in MS16-064.

CVE ID: CVE-2016-1104
Severity: IMPORTANT
Description: Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libra ries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vector s, a different vulnerability than other CVEs listed in MS16-064.

CVE ID: CVE-2016-1105
Severity: IMPORTANT
Description: Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libra ries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vector s, a different vulnerability than other CVEs listed in MS16-064.

CVE ID: CVE-2016-1106
Severity: IMPORTANT
Description: Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libra ries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vector s, a different vulnerability than other CVEs listed in MS16-064.

CVE ID: CVE-2016-1107
Severity: IMPORTANT
Description: Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libra ries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vector s, a different vulnerability than other CVEs listed in MS16-064.

CVE ID: CVE-2016-1108
Severity: IMPORTANT
Description: Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libra ries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vector s, a different vulnerability than other CVEs listed in MS16-064.

CVE ID: CVE-2016-1109
Severity: IMPORTANT
Description: Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libra ries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vector s, a different vulnerability than other CVEs listed in MS16-064.

CVE ID: CVE-2016-1110
Severity: IMPORTANT
Description: Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libra ries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vector s, a different vulnerability than other CVEs listed in MS16-064.

CVE ID: CVE-2016-3243
Severity: IMPORTANT
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a deni al of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vuln erability."

CVE ID: CVE-2016-3277
Severity: LOW
Description: Microsoft Internet Explorer 10 and 11 and Microsoft Edge allow remote attackers to obtain sensitive info rmation via a crafted web site, aka "Microsoft Browser Information Disclosure Vulnerability."

CVE ID: CVE-2016-3292

Severity: MODERATE
Description: Microsoft Internet Explorer 10 and 11 mishandles integrity settings and zone settings, which allows rem ote attackers to bypass a sandbox protection mechanism via a crafted web site, aka "Internet Explorer E levation of Privilege Vulnerability."

CVE ID: CVE-2016-3295
Severity: MODERATE
Description: Microsoft Internet Explorer 10 and 11 and Microsoft Edge allow remote attackers to execute arbitrary co de or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Mem ory Corruption Vulnerability."

CVE ID: CVE-2016-3321
Severity: LOW
Description: Microsoft Internet Explorer 10 and 11 load different files for attempts to open a file:// URL depending on whether the file exists, which allows local users to enumerate files via vectors involving a file:// URL and an HTML5 sandbox iframe, aka "Internet Explorer Information Disclosure Vulnerability."

CVE ID: CVE-2016-3383
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a deni al of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vul nerability."

CVE ID: CVE-2016-3387
Severity: IMPORTANT
Description: Microsoft Internet Explorer 10 and 11 and Microsoft Edge do not properly restrict access to private nam espaces, which allows remote attackers to gain privileges via unspecified vectors, aka "Microsoft Brows er Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-3388.

CVE ID: CVE-2016-3388
Severity: LOW
Description: Microsoft Internet Explorer 10 and 11 and Microsoft Edge do not properly restrict access to private nam espaces, which allows remote attackers to gain privileges via unspecified vectors, aka "Microsoft Brows er Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-3387.

CVE ID: CVE-2016-3391
Severity: LOW
Description: Microsoft Internet Explorer 10 and 11 and Microsoft Edge allow context-dependent attackers to discove r credentials by leveraging access to a memory dump, aka "Microsoft Browser Information Disclosure V ulnerability."

CVE ID: CVE-2016-4108
Severity: IMPORTANT
Description: Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libra ries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vector s, a different vulnerability than other CVEs listed in MS16-064.

CVE ID: CVE-2016-4109
Severity: IMPORTANT
Description: Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libra ries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vector s, a different vulnerability than other CVEs listed in MS16-064.

CVE ID: CVE-2016-4110
Severity: IMPORTANT
Description: Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libra ries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vector s, a different vulnerability than other CVEs listed in MS16-064.

CVE ID: CVE-2016-4111
Severity: IMPORTANT
Description: Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libra ries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vector s, a different vulnerability than other CVEs listed in MS16-064.

CVE ID: CVE-2016-4112
Severity: IMPORTANT
Description: Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libra

ries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vector s, a different vulnerability than other CVEs listed in MS16-064.

CVE ID: CVE-2016-4113
Severity: IMPORTANT
Description: Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libra ries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vector s, a different vulnerability than other CVEs listed in MS16-064.

CVE ID: CVE-2016-4114
Severity: IMPORTANT
Description: Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libra ries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vector s, a different vulnerability than other CVEs listed in MS16-064.

CVE ID: CVE-2016-4115
Severity: IMPORTANT
Description: Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libra ries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vector s, a different vulnerability than other CVEs listed in MS16-064.

CVE ID: CVE-2016-4116
Severity: IMPORTANT
Description: Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libra ries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vector s, a different vulnerability than other CVEs listed in MS16-064.

CVE ID: CVE-2016-7196
Severity: IMPORTANT
Description: Microsoft Internet Explorer 10 and 11 and Microsoft Edge allow remote attackers to execute arbitrary co de or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Mem ory Corruption Vulnerability."

CVE ID: CVE-2016-7281
Severity: LOW
Description: The Web Workers implementation in Microsoft Internet Explorer 10 and 11 and Microsoft Edge allows r emote attackers to bypass the Same Origin Policy via unspecified vectors, aka "Microsoft Browser Secu rity Feature Bypass Vulnerability."

CVE ID: CVE-2016-7284
Severity: MODERATE
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to obtain sensitive information from proce ss memory via a crafted web site, aka "Internet Explorer Information Disclosure Vulnerability."

CVE ID: CVE-2014-0267
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-0289 and CVE-2014-0290.

CVE ID: CVE-2014-0289
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-0267 and CVE-2014-0290.

CVE ID: CVE-2014-0290
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-0267 and CVE-2014-0289.

CVE ID: CVE-2014-0304
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability. "

CVE ID: CVE-2014-1760

Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability. "

CVE ID: CVE-2014-1769
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-1782, CVE-2014-1785, CVE-2014-2753, CVE-2014-2755, CVE -2014-2760, CVE-2014-2761, CVE-2014-2772, and CVE-2014-2776.

CVE ID: CVE-2014-1782
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-1769, CVE-2014-1785, CVE-2014-2753, CVE-2014-2755, CVE -2014-2760, CVE-2014-2761, CVE-2014-2772, and CVE-2014-2776.

CVE ID: CVE-2014-1785
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-1769, CVE-2014-1782, CVE-2014-2753, CVE-2014-2755, CVE -2014-2760, CVE-2014-2761, CVE-2014-2772, and CVE-2014-2776.

CVE ID: CVE-2014-2753
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-1769, CVE-2014-1782, CVE-2014-1785, CVE-2014-2755, CVE -2014-2760, CVE-2014-2761, CVE-2014-2772, and CVE-2014-2776.

CVE ID: CVE-2014-2755
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-1769, CVE-2014-1782, CVE-2014-1785, CVE-2014-2753, CVE -2014-2760, CVE-2014-2761, CVE-2014-2772, and CVE-2014-2776.

CVE ID: CVE-2014-2760
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-1769, CVE-2014-1782, CVE-2014-1785, CVE-2014-2753, CVE -2014-2755, CVE-2014-2761, CVE-2014-2772, and CVE-2014-2776.

CVE ID: CVE-2014-2761
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-1769, CVE-2014-1782, CVE-2014-1785, CVE-2014-2753, CVE -2014-2755, CVE-2014-2760, CVE-2014-2772, and CVE-2014-2776.

CVE ID: CVE-2014-2772
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-1769, CVE-2014-1782, CVE-2014-1785, CVE-2014-2753, CVE -2014-2755, CVE-2014-2760, CVE-2014-2761, and CVE-2014-2776.

CVE ID: CVE-2014-2776
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-1769, CVE-2014-1782, CVE-2014-1785, CVE-2014-2753, CVE -2014-2755, CVE-2014-2760, CVE-2014-2761, and CVE-2014-2772.

CVE ID: CVE-2014-2787

Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-2790, CVE-2014-2802, and CVE-2014-2806.

CVE ID: CVE-2014-2790
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-2787, CVE-2014-2802, and CVE-2014-2806.

CVE ID: CVE-2014-2802
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-2787, CVE-2014-2790, and CVE-2014-2806.

CVE ID: CVE-2014-2806
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-2787, CVE-2014-2790, and CVE-2014-2802.

CVE ID: CVE-2014-2810
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-2811, CVE-2014-2822, CVE-2014-2823, and CVE-2014-4057.

CVE ID: CVE-2014-2811
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-2810, CVE-2014-2822, CVE-2014-2823, and CVE-2014-4057.

CVE ID: CVE-2014-2822
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-2810, CVE-2014-2811, CVE-2014-2823, and CVE-2014-4057.

CVE ID: CVE-2014-2823
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-2810, CVE-2014-2811, CVE-2014-2822, and CVE-2014-4057.

CVE ID: CVE-2014-4057
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-2810, CVE-2014-2811, CVE-2014-2822, and CVE-2014-2823.

CVE ID: CVE-2014-4087
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-4095, CVE-2014-4096, and CVE-2014-4101.

CVE ID: CVE-2014-4095
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-4087, CVE-2014-4096, and CVE-2014-4101.

CVE ID: CVE-2014-4096
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se

rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-4087, CVE-2014-4095, and CVE-2014-4101.

CVE ID: CVE-2014-4101
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-4087, CVE-2014-4095, and CVE-2014-4096.

CVE ID: CVE-2014-4130
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-4132 and CVE-2014-4138.

CVE ID: CVE-2014-4132
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-4130 and CVE-2014-4138.

CVE ID: CVE-2014-4138
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-4130 and CVE-2014-4132.

CVE ID: CVE-2014-6327
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-6329 and CVE-2014-6376.

CVE ID: CVE-2014-6329
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-6327 and CVE-2014-6376.

CVE ID: CVE-2014-6347
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability. "

CVE ID: CVE-2014-6368
Severity: MODERATE
Description: Microsoft Internet Explorer 11 allows remote attackers to bypass the ASLR protection mechanism via a crafted web site, aka "Internet Explorer ASLR Bypass Vulnerability."

CVE ID: CVE-2014-6376
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-6327 and CVE-2014-6329.

CVE ID: CVE-2015-0018
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2015-0037, CVE-2015-0040, and CVE-2015-0066.

CVE ID: CVE-2015-0037
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2015-0018, CVE-2015-0040, and CVE-2015-0066.

CVE ID: CVE-2015-0040

Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2015-0018, CVE-2015-0037, and CVE-2015-0066.

CVE ID: CVE-2015-0056
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2015-1623 and CVE-2015-1626.

CVE ID: CVE-2015-0066
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2015-0018, CVE-2015-0037, and CVE-2015-0040.

CVE ID: CVE-2015-1623
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2015-0056 and CVE-2015-1626.

CVE ID: CVE-2015-1626
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2015-0056 and CVE-2015-1623.

CVE ID: CVE-2015-1658
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2015-1706, CVE-2015-1711, CVE-2015-1717, and CVE-2015-1718.

CVE ID: CVE-2015-1659
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2015-1662 and CVE-2015-1665.

CVE ID: CVE-2015-1662
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2015-1659 and CVE-2015-1665.

CVE ID: CVE-2015-1665
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2015-1659 and CVE-2015-1662.

CVE ID: CVE-2015-1685
Severity: MODERATE
Description: Microsoft Internet Explorer 11 allows remote attackers to bypass the ASLR protection mechanism via a crafted web site, aka "Internet Explorer ASLR Bypass."

CVE ID: CVE-2015-1706
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2015-1658, CVE-2015-1711, CVE-2015-1717, and CVE-2015-1718.

CVE ID: CVE-2015-1711
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability,

" a different vulnerability than CVE-2015-1658, CVE-2015-1706, CVE-2015-1717, and CVE-2015-1718.

CVE ID: CVE-2015-1713
Severity: IMPORTANT
Description: Microsoft Internet Explorer 11 allows remote attackers to gain privileges via a crafted web site, aka "Internet Explorer Elevation of Privilege Vulnerability."

CVE ID: CVE-2015-1717
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1658, CVE-2015-1706, CVE-2015-1711, and CVE-2015-1718.

CVE ID: CVE-2015-1718
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1658, CVE-2015-1706, CVE-2015-1711, and CVE-2015-1717.

CVE ID: CVE-2015-1732
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1742, CVE-2015-1747, CVE-2015-1750, and CVE-2015-1753.

CVE ID: CVE-2015-1742
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1732, CVE-2015-1747, CVE-2015-1750, and CVE-2015-1753.

CVE ID: CVE-2015-1747
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1732, CVE-2015-1742, CVE-2015-1750, and CVE-2015-1753.

CVE ID: CVE-2015-1750
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1732, CVE-2015-1742, CVE-2015-1747, and CVE-2015-1753.

CVE ID: CVE-2015-1753
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1732, CVE-2015-1742, CVE-2015-1747, and CVE-2015-1750.

CVE ID: CVE-2015-2383
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-2384 and CVE-2015-2425.

CVE ID: CVE-2015-2384
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-2383 and CVE-2015-2425.

CVE ID: CVE-2015-2425
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-2383 and CVE-2015-2384.

CVE ID: CVE-2015-2446

Severity: CRITICAL
Description: Microsoft Internet Explorer 11 and Edge allow remote attackers to execute arbitrary code or cause a de nial of service (memory corruption) via a crafted web site, aka "Memory Corruption Vulnerability," a diffe rent vulnerability than CVE-2015-2447.

CVE ID: CVE-2015-2447
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Memory Corruption Vulnerability," a different vuln erability than CVE-2015-2446.

CVE ID: CVE-2015-2489
Severity: MODERATE
Description: Microsoft Internet Explorer 11 allows remote attackers to gain privileges via a crafted web site, as demo nstrated by a transition from Low Integrity to Medium Integrity, aka "Elevation of Privilege Vulnerability."

CVE ID: CVE-2015-6042
Severity: CRITICAL
Description: Use-after-free vulnerability in the CWindow object implementation in Microsoft Internet Explorer 11 allo ws remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a cra fted web site, aka "Internet Explorer Memory Corruption Vulnerability."

CVE ID: CVE-2015-6045
Severity: CRITICAL
Description: Use-after-free vulnerability in the CElement object implementation in Microsoft Internet Explorer 11 allo ws remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via craft ed JavaScript that improperly interacts with use of the Cascading Style Sheets (CSS) empty-cells prope rty for a TABLE element, aka "Internet Explorer Memory Corruption Vulnerability."

CVE ID: CVE-2015-6053
Severity: MODERATE
Description: Microsoft Internet Explorer 11 allows remote attackers to obtain sensitive information from process me mory via crafted parameters in an ArrayBuffer.slice call, aka "Internet Explorer Information Disclosure V ulnerability."

CVE ID: CVE-2015-6068
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2015-6072, CVE-2015-6073, CVE-2015-6075, CVE-2015-6077, CVE -2015-6079, CVE-2015-6080, and CVE-2015-6082.

CVE ID: CVE-2015-6072
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2015-6068, CVE-2015-6073, CVE-2015-6075, CVE-2015-6077, CVE -2015-6079, CVE-2015-6080, and CVE-2015-6082.

CVE ID: CVE-2015-6073
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or c ause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Cor ruption Vulnerability," a different vulnerability than CVE-2015-6068, CVE-2015-6072, CVE-2015-6075, C VE-2015-6077, CVE-2015-6079, CVE-2015-6080, and CVE-2015-6082.

CVE ID: CVE-2015-6075
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2015-6068, CVE-2015-6072, CVE-2015-6073, CVE-2015-6077, CVE -2015-6079, CVE-2015-6080, and CVE-2015-6082.

CVE ID: CVE-2015-6077
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability,

" a different vulnerability than CVE-2015-6068, CVE-2015-6072, CVE-2015-6073, CVE-2015-6075, CVE-2015-6079, CVE-2015-6080, and CVE-2015-6082.

CVE ID: CVE-2015-6079
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-6068, CVE-2015-6072, CVE-2015-6073, CVE-2015-6075, CVE-2015-6077, CVE-2015-6080, and CVE-2015-6082.

CVE ID: CVE-2015-6080
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-6068, CVE-2015-6072, CVE-2015-6073, CVE-2015-6075, CVE-2015-6077, CVE-2015-6079, and CVE-2015-6082.

CVE ID: CVE-2015-6082
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-6068, CVE-2015-6072, CVE-2015-6073, CVE-2015-6075, CVE-2015-6077, CVE-2015-6079, and CVE-2015-6080.

CVE ID: CVE-2015-6139
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 and Microsoft Edge mishandle content types, which allows remote attackers to execute arbitrary web script in a privileged context via a crafted web site, aka "Microsoft Browser Elevation of Privilege Vulnerability."

CVE ID: CVE-2015-6140
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability," a different vulnerability than CVE-2015-6142, CVE-2015-6143, CVE-2015-6153, CVE-2015-6158, CVE-2015-6159, and CVE-2015-6160.

CVE ID: CVE-2015-6142
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability," a different vulnerability than CVE-2015-6140, CVE-2015-6143, CVE-2015-6153, CVE-2015-6158, CVE-2015-6159, and CVE-2015-6160.

CVE ID: CVE-2015-6143
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-6140, CVE-2015-6142, CVE-2015-6153, CVE-2015-6158, CVE-2015-6159, and CVE-2015-6160.

CVE ID: CVE-2015-6153
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability," a different vulnerability than CVE-2015-6140, CVE-2015-6142, CVE-2015-6143, CVE-2015-6158, CVE-2015-6159, and CVE-2015-6160.

CVE ID: CVE-2015-6157
Severity: MODERATE
Description: Microsoft Internet Explorer 11 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka "Internet Explorer Information Disclosure Vulnerability."

CVE ID: CVE-2015-6158
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability," a different vulnerability than CVE-2015-6140, CVE-2015-6142, CVE-2015-6143, C

VE-2015-6153, CVE-2015-6159, and CVE-2015-6160.

CVE ID: CVE-2015-6159
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or c ause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Cor ruption Vulnerability," a different vulnerability than CVE-2015-6140, CVE-2015-6142, CVE-2015-6143, C VE-2015-6153, CVE-2015-6158, and CVE-2015-6160.

CVE ID: CVE-2015-6160
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2015-6140, CVE-2015-6142, CVE-2015-6143, CVE-2015-6153, CVE -2015-6158, and CVE-2015-6159.

CVE ID: CVE-2016-0062
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or c ause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Cor ruption Vulnerability."

CVE ID: CVE-2016-0102
Severity: IMPORTANT
Description: Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or c ause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Cor ruption Vulnerability," a different vulnerability than CVE-2016-0103, CVE-2016-0106, CVE-2016-0108, C VE-2016-0109, and CVE-2016-0114.

CVE ID: CVE-2016-0103
Severity: IMPORTANT
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2016-0102, CVE-2016-0106, CVE-2016-0108, CVE-2016-0109, and CVE-2016-0114.

CVE ID: CVE-2016-0106
Severity: IMPORTANT
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2016-0102, CVE-2016-0103, CVE-2016-0108, CVE-2016-0109, and CVE-2016-0114.

CVE ID: CVE-2016-0108
Severity: IMPORTANT
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2016-0102, CVE-2016-0103, CVE-2016-0106, CVE-2016-0109, and CVE-2016-0114.

CVE ID: CVE-2016-0109
Severity: IMPORTANT
Description: Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or c ause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Cor ruption Vulnerability," a different vulnerability than CVE-2016-0102, CVE-2016-0103, CVE-2016-0106, C VE-2016-0108, and CVE-2016-0114.

CVE ID: CVE-2016-0114
Severity: IMPORTANT
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2016-0102, CVE-2016-0103, CVE-2016-0106, CVE-2016-0108, and CVE-2016-0109.

CVE ID: CVE-2016-0160
Severity: IMPORTANT
Description: Microsoft Internet Explorer 11 mishandles DLL loading, which allows local users to gain privileges via a crafted application, aka "DLL Loading Remote Code Execution Vulnerability."

CVE ID: CVE-2016-0166
Severity: IMPORTANT
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability. "

CVE ID: CVE-2016-0188
Severity: CRITICAL
Description: The User Mode Code Integrity (UMCI) implementation in Device Guard in Microsoft Internet Explorer 1 1 allows remote attackers to bypass a code-signing protection mechanism via unspecified vectors, aka " Internet Explorer Security Feature Bypass."

CVE ID: CVE-2016-3210
Severity: CRITICAL
Description: The Microsoft (1) JScript and (2) VBScript engines, as used in Internet Explorer 11, allow remote attack ers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, ak a "Scripting Engine Memory Corruption Vulnerability."

CVE ID: CVE-2016-3247
Severity: MODERATE
Description: Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or c ause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Cor ruption Vulnerability."

CVE ID: CVE-2016-3260
Severity: CRITICAL
Description: The Microsoft (1) JScript 9, (2) VBScript, and (3) Chakra JavaScript engines, as used in Microsoft Inter net Explorer 11, Microsoft Edge, and other products, allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Cor ruption Vulnerability."

CVE ID: CVE-2016-3261
Severity: LOW
Description: Microsoft Internet Explorer 11 allows remote attackers to obtain sensitive information via a crafted web site, aka "Internet Explorer Information Disclosure Vulnerability."

CVE ID: CVE-2016-3276
Severity: LOW
Description: Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to conduct content-spoofing a ttacks via a crafted URL, aka "Microsoft Browser Spoofing Vulnerability."

CVE ID: CVE-2016-3288
Severity: IMPORTANT
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code via a crafted web page, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3290.

CVE ID: CVE-2016-3289
Severity: IMPORTANT
Description: Microsoft Internet Explorer 11 and Edge allow remote attackers to execute arbitrary code via a crafted web page, aka "Microsoft Browser Memory Corruption Vulnerability," a different vulnerability than CVE-2 016-3322.

CVE ID: CVE-2016-3290
Severity: IMPORTANT
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code via a crafted web page, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3288.

CVE ID: CVE-2016-3291
Severity: LOW
Description: Microsoft Internet Explorer 11 and Microsoft Edge mishandle cross-origin requests, which allows remot e attackers to obtain sensitive information via a crafted web site, aka "Microsoft Browser Information Dis closure Vulnerability."

CVE ID: CVE-2016-3322
Severity: IMPORTANT
Description: Microsoft Internet Explorer 11 and Edge allow remote attackers to execute arbitrary code via a crafted web page, aka "Microsoft Browser Memory Corruption Vulnerability," a different vulnerability than CVE-2

016-3289.

CVE ID: CVE-2016-3325
Severity: LOW
Description: Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to obtain sensitive information via a crafted web site, aka "Microsoft Browser Information Disclosure Vulnerability."

CVE ID: CVE-2016-3331
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or c ause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Cor ruption Vulnerability."

CVE ID: CVE-2016-3390
Severity: IMPORTANT
Description: The scripting engines in Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to ex ecute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, as demonst rated by the Chakra JavaScript engine, aka "Scripting Engine Memory Corruption Vulnerability."

CVE ID: CVE-2016-7241
Severity: IMPORTANT
Description: Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or c ause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Cor ruption Vulnerability."

CVE ID: CVE-2016-7287
Severity: IMPORTANT
Description: The scripting engines in Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to ex ecute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripti ng Engine Memory Corruption Vulnerability."

CVE ID: CVE-2017-0037
Severity: IMPORTANT
Description: Microsoft Internet Explorer 10 and 11 and Microsoft Edge have a type confusion issue in the Layout::M ultiColumnBoxBuilder::HandleColumnBreakOnColumnSpanningElement function in mshtml.dll, which all ows remote attackers to execute arbitrary code via vectors involving a crafted Cascading Style Sheets (CSS) token sequence and crafted JavaScript code that operates on a TH element.

CVE ID: CVE-2017-0008
Severity: MODERATE
Description: Microsoft Internet Explorer 9 through 11 allow remote attackers to obtain sensitive information from pro cess memory via a crafted web site, aka "Internet Explorer Information Disclosure Vulnerability." This vu lnerability is different from those described in CVE-2017-0009 and CVE-2017-0059.

CVE ID: CVE-2017-0009
Severity: MODERATE
Description: Microsoft Internet Explorer 9 through 11 allow remote attackers to obtain sensitive information from pro cess memory via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability." This vuln erability is different from those described in CVE-2017-0011, CVE-2017-0017, CVE-2017-0065, and CV E-2017-0068.

CVE ID: CVE-2017-0040
Severity: IMPORTANT
Description: The scripting engine in Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbi trary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability." This vulnerability is different from that described in CVE-2017-0130.

CVE ID: CVE-2017-0059
Severity: MODERATE
Description: Microsoft Internet Explorer 9 through 11 allow remote attackers to obtain sensitive information from pro cess memory via a crafted web site, aka "Internet Explorer Information Disclosure Vulnerability." This vu lnerability is different from those described in CVE-2017-0008 and CVE-2017-0009.

CVE ID: CVE-2017-0130
Severity: IMPORTANT
Description: The scripting engine in Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbi trary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability." This vulnerability is different from that described in CVE-2017-0040.

CVE ID: CVE-2017-0149
Severity: IMPORTANT
Description: Microsoft Internet Explorer 9 through 11 allow remote attackers to execute arbitrary code or cause a de nial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vul nerability." This vulnerability is different from those described in CVE-2017-0018 and CVE-2017-0037.

CVE ID: CVE-2017-0018
Severity: IMPORTANT
Description: Microsoft Internet Explorer 10 and 11 allow remote attackers to execute arbitrary code or cause a denia l of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulner ability." This vulnerability is different from those described in CVE-2017-0037 and CVE-2017-0149.

CVE ID: CVE-2017-0012
Severity: MODERATE
Description: Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to spoof web content via a cr afted web site, aka "Microsoft Browser Spoofing Vulnerability." This vulnerability is different from those d escribed in CVE-2017-0033 and CVE-2017-0069.

CVE ID: CVE-2017-0033
Severity: MODERATE
Description: Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to spoof web content via a cr afted web site, aka "Microsoft Browser Spoofing Vulnerability." This vulnerability is different from those d escribed in CVE-2017-0012 and CVE-2017-0069.

CVE ID: CVE-2017-0049
Severity: MODERATE
Description: The VBScript engine in Microsoft Internet Explorer 11 allows remote attackers to obtain sensitive inform ation from process memory via a crafted web site, aka "Scripting Engine Information Disclosure Vulnera bility." This vulnerability is different from those described in CVE-2017-0018, and CVE-2017-0037.

CVE ID: CVE-2017-0154
Severity: MODERATE
Description: Microsoft Internet Explorer 11 on Windows 10, 1511, and 1606 and Windows Server 2016 does not enf orce cross-domain policies, allowing attackers to access information from one domain and inject it into a nother via a crafted application, aka, "Internet Explorer Elevation of Privilege Vulnerability."

CVE ID: CVE-2017-0210
Severity: MODERATE
Description: An elevation of privilege vulnerability exists when Internet Explorer does not properly enforce cross-do main policies, which could allow an attacker to access information from one domain and inject it into ano ther domain, aka "Internet Explorer Elevation of Privilege Vulnerability."

CVE ID: CVE-2017-0202
Severity: IMPORTANT
Description: A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in me mory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary cod e in the context of the current user, a.k.a. "Internet Explorer Memory Corruption Vulnerability."

Internet Explorer 11.0.9600.18282 (update available)

CVE ID: CVE-2013-3893
Severity: CRITICAL
Description: Use-after-free vulnerability in the SetMouseCapture implementation in mshtml.dll in Microsoft Internet E xplorer 6 through 11 allows remote attackers to execute arbitrary code via crafted JavaScript strings, as demonstrated by use of an ms-help: URL that triggers loading of hxds.dll.

CVE ID: CVE-2013-3897
Severity: CRITICAL
Description: Use-after-free vulnerability in the CDisplayPointer class in mshtml.dll in Microsoft Internet Explorer 6 thr ough 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corrupti on) via crafted JavaScript code that uses the onpropertychange event handler, as exploited in the wild in September and October 2013, aka "Internet Explorer Memory Corruption Vulnerability."

CVE ID: CVE-2013-3915
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V

ulnerability," a different vulnerability than CVE-2013-3917.

CVE ID: CVE-2013-3917
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2013-3915.

CVE ID: CVE-2013-5047
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2013-5048.

CVE ID: CVE-2013-5048
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2013-5047.

CVE ID: CVE-2013-7331
Severity: MODERATE
Description: The Microsoft.XMLDOM ActiveX control in Microsoft Windows 8.1 and earlier allows remote attackers t o determine the existence of local pathnames, UNC share pathnames, intranet hostnames, and intranet IP addresses by examining error codes, as demonstrated by a res:// URL, and exploited in the wild in Fe bruary 2014.

CVE ID: CVE-2014-0271
Severity: CRITICAL
Description: The VBScript engine in Microsoft Internet Explorer 6 through 11, and VBScript 5.6 through 5.8, allows r emote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "VBScript Memory Corruption Vulnerability."

CVE ID: CVE-2014-0275
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-0285 and CVE-2014-0286.

CVE ID: CVE-2014-0282
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-1775, CVE-2014-1779, CVE-2014-1799, CVE-2014 -1803, and CVE-2014-2757.

CVE ID: CVE-2014-0285
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-0275 and CVE-2014-0286.

CVE ID: CVE-2014-0286
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-0275 and CVE-2014-0285.

CVE ID: CVE-2014-0299
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-0305 and CVE-2014-0311.

CVE ID: CVE-2014-0305
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V

ulnerability," a different vulnerability than CVE-2014-0299 and CVE-2014-0311.

CVE ID: CVE-2014-0310
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-1815.

CVE ID: CVE-2014-0311
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-0299 and CVE-2014-0305.

CVE ID: CVE-2014-1762
Severity: IMPORTANT
Description: Unspecified vulnerability in Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code with medium-integrity privileges and bypass a sandbox protection mechanism via unknow n vectors, as demonstrated by ZDI during a Pwn4Fun competition at CanSecWest 2014.

CVE ID: CVE-2014-1765
Severity: IMPORTANT
Description: Multiple use-after-free vulnerabilities in Microsoft Internet Explorer 6 through 11 allow remote attackers to execute arbitrary code via unspecified vectors, as demonstrated by Sebastian Apelt and Andreas Sch midt during a Pwn2Own competition at CanSecWest 2014.

CVE ID: CVE-2014-1770
Severity: CRITICAL
Description: Use-after-free vulnerability in Microsoft Internet Explorer 6 through 11 allows remote attackers to execut e arbitrary code via crafted JavaScript code that interacts improperly with a CollectGarbage function call on a CMarkup object allocated by the CMarkup::CreateInitialMarkup function.

CVE ID: CVE-2014-1771
Severity: IMPORTANT
Description: SChannel in Microsoft Internet Explorer 6 through 11 does not ensure that a server’s X.509 certificate is the same during renegotiation as it was before renegotiation, which allows man-in-the-middle attackers t o obtain sensitive information or modify TLS session data via a "triple handshake attack," aka "TLS Serv er Certificate Renegotiation Vulnerability."

CVE ID: CVE-2014-1775
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-0282, CVE-2014-1779, CVE-2014-1799, CVE-2014 -1803, and CVE-2014-2757.

CVE ID: CVE-2014-1776
Severity: CRITICAL
Description: Use-after-free vulnerability in Microsoft Internet Explorer 6 through 11 allows remote attackers to execut e arbitrary code or cause a denial of service (memory corruption) via vectors related to the CMarkup::Is ConnectedToPrimaryMarkup function, as exploited in the wild in April 2014. NOTE: this issue originally emphasized VGX.DLL, but Microsoft clarified that "VGX.DLL does not contain the vulnerable code lever aged in this exploit. Disabling VGX.DLL is an exploit-specific workaround that provides an immediate, ef fective workaround to help block known attacks."

CVE ID: CVE-2014-1779
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-0282, CVE-2014-1775, CVE-2014-1799, CVE-2014 -1803, and CVE-2014-2757.

CVE ID: CVE-2014-1796
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 and 8 through 11 allows remote attackers to execute arbitrary code or cau se a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corrupt ion Vulnerability."

CVE ID: CVE-2014-1799

Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-0282, CVE-2014-1775, CVE-2014-1779, CVE-2014-1803, and CVE-2014-2757.

CVE ID: CVE-2014-1803
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-0282, CVE-2014-1775, CVE-2014-1779, CVE-2014-1799, and CVE-2014-2757.

CVE ID: CVE-2014-1815
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, as exploited in the wild in May 2014, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-0310.

CVE ID: CVE-2014-2757
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-0282, CVE-2014-1775, CVE-2014-1779, CVE-2014-1799, and CVE-2014-1803.

CVE ID: CVE-2014-2774
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-2820, CVE-2014-2826, CVE-2014-2827, and CVE-2014-4063.

CVE ID: CVE-2014-2799
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-4059, CVE-2014-4065, CVE-2014-4079, CVE-2014-4081, CVE-2014-4083, CVE-2014-4085, CVE-2014-4088, CVE-2014-4090, CVE-2014-4094, CVE-2014-4097, CVE-2014-4100, CVE-2014-4103, CVE-2014-4104, CVE-2014-4105, CVE-2014-4106, CVE-2014-4107, CVE-2014-4108, CVE-2014-4109, CVE-2014-4110, and CVE-2014-4111.

CVE ID: CVE-2014-2800
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-2807 and CVE-2014-2809.

CVE ID: CVE-2014-2807
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-2800 and CVE-2014-2809.

CVE ID: CVE-2014-2809
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-2800 and CVE-2014-2807.

CVE ID: CVE-2014-2817
Severity: IMPORTANT
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to gain privileges via a crafted web site, aka "Internet Explorer Elevation of Privilege Vulnerability."

CVE ID: CVE-2014-2820
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d

enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-2774, CVE-2014-2826, CVE-2014-2827, and CVE-2014-4063.

CVE ID: CVE-2014-2826
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-2774, CVE-2014-2820, CVE-2014-2827, and CVE-2014-4063.

CVE ID: CVE-2014-2827
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-2774, CVE-2014-2820, CVE-2014-2826, and CVE-2014-4063.

CVE ID: CVE-2014-4059
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-2799, CVE-2014-4065, CVE-2014-4079, CVE-2014 -4081, CVE-2014-4083, CVE-2014-4085, CVE-2014-4088, CVE-2014-4090, CVE-2014-4094, CVE-201 4-4097, CVE-2014-4100, CVE-2014-4103, CVE-2014-4104, CVE-2014-4105, CVE-2014-4106, CVE-20 14-4107, CVE-2014-4108, CVE-2014-4109, CVE-2014-4110, and CVE-2014-4111.

CVE ID: CVE-2014-4063
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-2774, CVE-2014-2820, CVE-2014-2826, and CVE-2014-2827.

CVE ID: CVE-2014-4065
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-2799, CVE-2014-4059, CVE-2014-4079, CVE-2014 -4081, CVE-2014-4083, CVE-2014-4085, CVE-2014-4088, CVE-2014-4090, CVE-2014-4094, CVE-201 4-4097, CVE-2014-4100, CVE-2014-4103, CVE-2014-4104, CVE-2014-4105, CVE-2014-4106, CVE-20 14-4107, CVE-2014-4108, CVE-2014-4109, CVE-2014-4110, and CVE-2014-4111.

CVE ID: CVE-2014-4079
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-2799, CVE-2014-4059, CVE-2014-4065, CVE-2014 -4081, CVE-2014-4083, CVE-2014-4085, CVE-2014-4088, CVE-2014-4090, CVE-2014-4094, CVE-201 4-4097, CVE-2014-4100, CVE-2014-4103, CVE-2014-4104, CVE-2014-4105, CVE-2014-4106, CVE-20 14-4107, CVE-2014-4108, CVE-2014-4109, CVE-2014-4110, and CVE-2014-4111.

CVE ID: CVE-2014-4081
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-2799, CVE-2014-4059, CVE-2014-4065, CVE-2014 -4079, CVE-2014-4083, CVE-2014-4085, CVE-2014-4088, CVE-2014-4090, CVE-2014-4094, CVE-201 4-4097, CVE-2014-4100, CVE-2014-4103, CVE-2014-4104, CVE-2014-4105, CVE-2014-4106, CVE-20 14-4107, CVE-2014-4108, CVE-2014-4109, CVE-2014-4110, and CVE-2014-4111.

CVE ID: CVE-2014-4083
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-2799, CVE-2014-4059, CVE-2014-4065, CVE-2014 -4079, CVE-2014-4081, CVE-2014-4085, CVE-2014-4088, CVE-2014-4090, CVE-2014-4094, CVE-201 4-4097, CVE-2014-4100, CVE-2014-4103, CVE-2014-4104, CVE-2014-4105, CVE-2014-4106, CVE-20 14-4107, CVE-2014-4108, CVE-2014-4109, CVE-2014-4110, and CVE-2014-4111.

CVE ID: CVE-2014-4085
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-2799, CVE-2014-4059, CVE-2014-4065, CVE-2014-4079, CVE-2014-4081, CVE-2014-4083, CVE-2014-4088, CVE-2014-4090, CVE-2014-4094, CVE-2014-4097, CVE-2014-4100, CVE-2014-4103, CVE-2014-4104, CVE-2014-4105, CVE-2014-4106, CVE-2014-4107, CVE-2014-4108, CVE-2014-4109, CVE-2014-4110, and CVE-2014-4111.

CVE ID: CVE-2014-4088
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-2799, CVE-2014-4059, CVE-2014-4065, CVE-2014-4079, CVE-2014-4081, CVE-2014-4083, CVE-2014-4085, CVE-2014-4090, CVE-2014-4094, CVE-2014-4097, CVE-2014-4100, CVE-2014-4103, CVE-2014-4104, CVE-2014-4105, CVE-2014-4106, CVE-2014-4107, CVE-2014-4108, CVE-2014-4109, CVE-2014-4110, and CVE-2014-4111.

CVE ID: CVE-2014-4090
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-2799, CVE-2014-4059, CVE-2014-4065, CVE-2014-4079, CVE-2014-4081, CVE-2014-4083, CVE-2014-4085, CVE-2014-4088, CVE-2014-4094, CVE-2014-4097, CVE-2014-4100, CVE-2014-4103, CVE-2014-4104, CVE-2014-4105, CVE-2014-4106, CVE-2014-4107, CVE-2014-4108, CVE-2014-4109, CVE-2014-4110, and CVE-2014-4111.

CVE ID: CVE-2014-4094
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-2799, CVE-2014-4059, CVE-2014-4065, CVE-2014-4079, CVE-2014-4081, CVE-2014-4083, CVE-2014-4085, CVE-2014-4088, CVE-2014-4090, CVE-2014-4097, CVE-2014-4100, CVE-2014-4103, CVE-2014-4104, CVE-2014-4105, CVE-2014-4106, CVE-2014-4107, CVE-2014-4108, CVE-2014-4109, CVE-2014-4110, and CVE-2014-4111.

CVE ID: CVE-2014-4097
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-2799, CVE-2014-4059, CVE-2014-4065, CVE-2014-4079, CVE-2014-4081, CVE-2014-4083, CVE-2014-4085, CVE-2014-4088, CVE-2014-4090, CVE-2014-4094, CVE-2014-4100, CVE-2014-4103, CVE-2014-4104, CVE-2014-4105, CVE-2014-4106, CVE-2014-4107, CVE-2014-4108, CVE-2014-4109, CVE-2014-4110, and CVE-2014-4111.

CVE ID: CVE-2014-4100
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-2799, CVE-2014-4059, CVE-2014-4065, CVE-2014-4079, CVE-2014-4081, CVE-2014-4083, CVE-2014-4085, CVE-2014-4088, CVE-2014-4090, CVE-2014-4094, CVE-2014-4097, CVE-2014-4103, CVE-2014-4104, CVE-2014-4105, CVE-2014-4106, CVE-2014-4107, CVE-2014-4108, CVE-2014-4109, CVE-2014-4110, and CVE-2014-4111.

CVE ID: CVE-2014-4103
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-2799, CVE-2014-4059, CVE-2014-4065, CVE-2014-4079, CVE-2014-4081, CVE-2014-4083, CVE-2014-4085, CVE-2014-4088, CVE-2014-4090, CVE-2014-4094, CVE-2014-4097, CVE-2014-4100, CVE-2014-4104, CVE-2014-4105, CVE-2014-4106, CVE-2014-4107, CVE-2014-4108, CVE-2014-4109, CVE-2014-4110, and CVE-2014-4111.

CVE ID: CVE-2014-4104
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-2799, CVE-2014-4059, CVE-2014-4065, CVE-2014

-4079, CVE-2014-4081, CVE-2014-4083, CVE-2014-4085, CVE-2014-4088, CVE-2014-4090, CVE-201
4-4094, CVE-2014-4097, CVE-2014-4100, CVE-2014-4103, CVE-2014-4105, CVE-2014-4106, CVE-20
14-4107, CVE-2014-4108, CVE-2014-4109, CVE-2014-4110, and CVE-2014-4111.

CVE ID: CVE-2014-4105
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d
enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V
ulnerability," a different vulnerability than CVE-2014-2799, CVE-2014-4059, CVE-2014-4065, CVE-2014
-4079, CVE-2014-4081, CVE-2014-4083, CVE-2014-4085, CVE-2014-4088, CVE-2014-4090, CVE-201
4-4094, CVE-2014-4097, CVE-2014-4100, CVE-2014-4103, CVE-2014-4104, CVE-2014-4106, CVE-20
14-4107, CVE-2014-4108, CVE-2014-4109, CVE-2014-4110, and CVE-2014-4111.

CVE ID: CVE-2014-4106
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d
enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V
ulnerability," a different vulnerability than CVE-2014-2799, CVE-2014-4059, CVE-2014-4065, CVE-2014
-4079, CVE-2014-4081, CVE-2014-4083, CVE-2014-4085, CVE-2014-4088, CVE-2014-4090, CVE-201
4-4094, CVE-2014-4097, CVE-2014-4100, CVE-2014-4103, CVE-2014-4104, CVE-2014-4105, CVE-20
14-4107, CVE-2014-4108, CVE-2014-4109, CVE-2014-4110, and CVE-2014-4111.

CVE ID: CVE-2014-4107
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d
enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V
ulnerability," a different vulnerability than CVE-2014-2799, CVE-2014-4059, CVE-2014-4065, CVE-2014
-4079, CVE-2014-4081, CVE-2014-4083, CVE-2014-4085, CVE-2014-4088, CVE-2014-4090, CVE-201
4-4094, CVE-2014-4097, CVE-2014-4100, CVE-2014-4103, CVE-2014-4104, CVE-2014-4105, CVE-20
14-4106, CVE-2014-4108, CVE-2014-4109, CVE-2014-4110, and CVE-2014-4111.

CVE ID: CVE-2014-4108
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d
enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V
ulnerability," a different vulnerability than CVE-2014-2799, CVE-2014-4059, CVE-2014-4065, CVE-2014
-4079, CVE-2014-4081, CVE-2014-4083, CVE-2014-4085, CVE-2014-4088, CVE-2014-4090, CVE-201
4-4094, CVE-2014-4097, CVE-2014-4100, CVE-2014-4103, CVE-2014-4104, CVE-2014-4105, CVE-20
14-4106, CVE-2014-4107, CVE-2014-4109, CVE-2014-4110, and CVE-2014-4111.

CVE ID: CVE-2014-4109
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d
enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V
ulnerability," a different vulnerability than CVE-2014-2799, CVE-2014-4059, CVE-2014-4065, CVE-2014
-4079, CVE-2014-4081, CVE-2014-4083, CVE-2014-4085, CVE-2014-4088, CVE-2014-4090, CVE-201
4-4094, CVE-2014-4097, CVE-2014-4100, CVE-2014-4103, CVE-2014-4104, CVE-2014-4105, CVE-20
14-4106, CVE-2014-4107, CVE-2014-4108, CVE-2014-4110, and CVE-2014-4111.

CVE ID: CVE-2014-4110
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d
enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V
ulnerability," a different vulnerability than CVE-2014-2799, CVE-2014-4059, CVE-2014-4065, CVE-2014
-4079, CVE-2014-4081, CVE-2014-4083, CVE-2014-4085, CVE-2014-4088, CVE-2014-4090, CVE-201
4-4094, CVE-2014-4097, CVE-2014-4100, CVE-2014-4103, CVE-2014-4104, CVE-2014-4105, CVE-20
14-4106, CVE-2014-4107, CVE-2014-4108, CVE-2014-4109, and CVE-2014-4111.

CVE ID: CVE-2014-4111
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d
enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V
ulnerability," a different vulnerability than CVE-2014-2799, CVE-2014-4059, CVE-2014-4065, CVE-2014
-4079, CVE-2014-4081, CVE-2014-4083, CVE-2014-4085, CVE-2014-4088, CVE-2014-4090, CVE-201
4-4094, CVE-2014-4097, CVE-2014-4100, CVE-2014-4103, CVE-2014-4104, CVE-2014-4105, CVE-20
14-4106, CVE-2014-4107, CVE-2014-4108, CVE-2014-4109, and CVE-2014-4110.

CVE ID: CVE-2014-4128
Severity: CRITICAL

Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability."

CVE ID: CVE-2014-4143
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-6341.

CVE ID: CVE-2014-6340
Severity: MODERATE
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to read content from a different (1) do main or (2) zone via a crafted web site, aka "Internet Explorer Cross-domain Information Disclosure Vul nerability."

CVE ID: CVE-2014-6341
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-4143.

CVE ID: CVE-2014-6363
Severity: CRITICAL
Description: vbscript.dll in Microsoft VBScript 5.6 through 5.8, as used with Internet Explorer 6 through 11 and other products, allows remote attackers to execute arbitrary code or cause a denial of service (memory corrup tion) via a crafted web site, aka "VBScript Memory Corruption Vulnerability."

CVE ID: CVE-2014-6374
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability."

CVE ID: CVE-2015-0017
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-0020, CVE-2015-0022, CVE-2015-0026, CVE-2015 -0030, CVE-2015-0031, CVE-2015-0036, and CVE-2015-0041.

CVE ID: CVE-2015-0020
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-0017, CVE-2015-0022, CVE-2015-0026, CVE-2015 -0030, CVE-2015-0031, CVE-2015-0036, and CVE-2015-0041.

CVE ID: CVE-2015-0022
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-0017, CVE-2015-0020, CVE-2015-0026, CVE-2015 -0030, CVE-2015-0031, CVE-2015-0036, and CVE-2015-0041.

CVE ID: CVE-2015-0026
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-0017, CVE-2015-0020, CVE-2015-0022, CVE-2015 -0030, CVE-2015-0031, CVE-2015-0036, and CVE-2015-0041.

CVE ID: CVE-2015-0030
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-0017, CVE-2015-0020, CVE-2015-0022, CVE-2015 -0026, CVE-2015-0031, CVE-2015-0036, and CVE-2015-0041.

CVE ID: CVE-2015-0031
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-0017, CVE-2015-0020, CVE-2015-0022, CVE-2015-0026, CVE-2015-0030, CVE-2015-0036, and CVE-2015-0041.

CVE ID: CVE-2015-0036
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-0017, CVE-2015-0020, CVE-2015-0022, CVE-2015-0026, CVE-2015-0030, CVE-2015-0031, and CVE-2015-0041.

CVE ID: CVE-2015-0041
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-0017, CVE-2015-0020, CVE-2015-0022, CVE-2015-0026, CVE-2015-0030, CVE-2015-0031, and CVE-2015-0036.

CVE ID: CVE-2015-0070
Severity: MODERATE
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to read content from a different (1) domain or (2) zone via a crafted web site, aka "Internet Explorer Cross-domain Information Disclosure Vulnerability."

CVE ID: CVE-2015-1625
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1634.

CVE ID: CVE-2015-1634
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1625.

CVE ID: CVE-2015-1652
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1666.

CVE ID: CVE-2015-1661
Severity: MODERATE
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to bypass the ASLR protection mechanism via a crafted web site, aka "Internet Explorer ASLR Bypass Vulnerability."

CVE ID: CVE-2015-1666
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1652.

CVE ID: CVE-2015-1694
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1710.

CVE ID: CVE-2015-1703
Severity: IMPORTANT
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to gain privileges via a crafted web site, aka "Internet Explorer Elevation of Privilege Vulnerability," a different vulnerability than CVE-2015-1704.

CVE ID: CVE-2015-1704
Severity: IMPORTANT
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to gain privileges via a crafted web sit e, aka "Internet Explorer Elevation of Privilege Vulnerability," a different vulnerability than CVE-2015-17 03.

CVE ID: CVE-2015-1710
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-1694.

CVE ID: CVE-2015-1735
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-1740, CVE-2015-1744, CVE-2015-1745, and CVE-2015-1766.

CVE ID: CVE-2015-1740
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-1735, CVE-2015-1744, CVE-2015-1745, and CVE-2015-1766.

CVE ID: CVE-2015-1744
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-1735, CVE-2015-1740, CVE-2015-1745, and CVE-2015-1766.

CVE ID: CVE-2015-1745
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-1735, CVE-2015-1740, CVE-2015-1744, and CVE-2015-1766.

CVE ID: CVE-2015-1766
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-1735, CVE-2015-1740, CVE-2015-1744, and CVE-2015-1745.

CVE ID: CVE-2015-2385
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-2390, CVE-2015-2397, CVE-2015-2404, CVE-2015 -2406, and CVE-2015-2422.

CVE ID: CVE-2015-2390
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-2385, CVE-2015-2397, CVE-2015-2404, CVE-2015 -2406, and CVE-2015-2422.

CVE ID: CVE-2015-2397
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-2385, CVE-2015-2390, CVE-2015-2404, CVE-2015 -2406, and CVE-2015-2422.

CVE ID: CVE-2015-2404
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-2385, CVE-2015-2390, CVE-2015-2397, CVE-2015-2406, and CVE-2015-2422.

CVE ID: CVE-2015-2406
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-2385, CVE-2015-2390, CVE-2015-2397, CVE-2015-2404, and CVE-2015-2422.

CVE ID: CVE-2015-2410
Severity: MODERATE
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to determine the existence of local files via a crafted stylesheet, aka "Internet Explorer Information Disclosure Vulnerability."

CVE ID: CVE-2015-2413
Severity: MODERATE
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to determine the existence of local files via a crafted module-resource request, aka "Internet Explorer Information Disclosure Vulnerability."

CVE ID: CVE-2015-2421
Severity: MODERATE
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to bypass the ASLR protection mechanism via a crafted web site, aka "Internet Explorer ASLR Bypass."

CVE ID: CVE-2015-2422
Severity: CRITICAL
Description: Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-2385, CVE-2015-2390, CVE-2015-2397, CVE-2015-2404, and CVE-2015-2406.

CVE ID: CVE-2013-5046
Severity: IMPORTANT
Description: Microsoft Internet Explorer 7 through 11 allows local users to bypass the Protected Mode protection mechanism, and consequently gain privileges, by leveraging the ability to execute sandboxed code, aka "Internet Explorer Elevation of Privilege Vulnerability."

CVE ID: CVE-2014-1764
Severity: CRITICAL
Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to execute arbitrary code and bypass a sandbox protection mechanism by leveraging "object confusion" in a broker process, as demonstrated by VUPEN during a Pwn2Own competition at CanSecWest 2014.

CVE ID: CVE-2014-1791
Severity: CRITICAL
Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability."

CVE ID: CVE-2014-2783
Severity: IMPORTANT
Description: Microsoft Internet Explorer 7 through 11 does not prevent use of wildcard EV SSL certificates, which might allow remote attackers to spoof a trust level by leveraging improper issuance of a wildcard certificate by a recognized Certification Authority, aka "Extended Validation (EV) Certificate Security Feature Bypass Vulnerability."

CVE ID: CVE-2014-2819
Severity: IMPORTANT
Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to gain privileges via a crafted web site, aka "Internet Explorer Elevation of Privilege Vulnerability."

CVE ID: CVE-2014-4056

Severity: CRITICAL
Description: Microsoft Internet Explorer 7 through 10 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability."

CVE ID: CVE-2014-4123
Severity: IMPORTANT
Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to gain privileges via a crafted web sit e, aka "Internet Explorer Elevation of Privilege Vulnerability," as exploited in the wild in October 2014, a different vulnerability than CVE-2014-4124.

CVE ID: CVE-2014-4124
Severity: IMPORTANT
Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to gain privileges via a crafted web sit e, aka "Internet Explorer Elevation of Privilege Vulnerability," a different vulnerability than CVE-2014-41 23.

CVE ID: CVE-2014-6323
Severity: MODERATE
Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to obtain sensitive clipboard informatio n via a crafted web site, aka "Internet Explorer Clipboard Information Disclosure Vulnerability."

CVE ID: CVE-2015-1627
Severity: MODERATE
Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to gain privileges via a crafted web sit e, aka "Internet Explorer Elevation of Privilege Vulnerability."

CVE ID: CVE-2015-1688
Severity: IMPORTANT
Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to gain privileges via a crafted web sit e, aka "Internet Explorer Elevation of Privilege Vulnerability."

CVE ID: CVE-2015-1692
Severity: MODERATE
Description: Microsoft Internet Explorer 7 through 11 allows user-assisted remote attackers to read the clipboard co ntents via crafted web script, aka "Internet Explorer Clipboard Information Disclosure Vulnerability."

CVE ID: CVE-2015-1709
Severity: CRITICAL
Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability."

CVE ID: CVE-2015-1743
Severity: IMPORTANT
Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to gain privileges via a crafted web sit e, aka "Internet Explorer Elevation of Privilege Vulnerability," a different vulnerability than CVE-2015-17 48.

CVE ID: CVE-2015-1748
Severity: IMPORTANT
Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to gain privileges via a crafted web sit e, aka "Internet Explorer Elevation of Privilege Vulnerability," a different vulnerability than CVE-2015-17 43.

CVE ID: CVE-2015-2402
Severity: MODERATE
Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to gain privileges via a crafted web sit e, aka "Internet Explorer Elevation of Privilege Vulnerability."

CVE ID: CVE-2015-2423
Severity: MODERATE
Description: Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, W indows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, Windows 10, Excel 2007 S P3, PowerPoint 2007 SP3, Visio 2007 SP3, Word 2007 SP3, Office 2010 SP2, Excel 2010 SP2, Power Point 2010 SP2, Visio 2010 SP2, Word 2010 SP2, Excel 2013 SP1, PowerPoint 2013 SP1, Visio 2013 SP1, Word 2013 SP1, Excel 2013 RT SP1, PowerPoint 2013 RT SP1, Visio 2013 RT SP1, Word 2013 RT SP1, and Internet Explorer 7 through 11 allow remote attackers to gain privileges and obtain sensitiv

e information via a crafted command-line parameter to an Office application or Notepad, as demonstrate d by a transition from Low Integrity to Medium Integrity, aka "Unsafe Command Line Parameter Passing Vulnerability."

CVE ID: CVE-2015-2441
Severity: CRITICAL
Description: Microsoft Internet Explorer 7 through 11 and Edge allow remote attackers to execute arbitrary code or c ause a denial of service (memory corruption) via a crafted web site, aka "Memory Corruption Vulnerabilit y," a different vulnerability than CVE-2015-2452.

CVE ID: CVE-2015-2449
Severity: MODERATE
Description: Microsoft Internet Explorer 7 through 11 and Edge allow remote attackers to bypass the ASLR protectio n mechanism via a crafted web site, aka "ASLR Bypass."

CVE ID: CVE-2015-2452
Severity: CRITICAL
Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Memory Corruption Vulnerability," a diff erent vulnerability than CVE-2015-2441.

CVE ID: CVE-2015-2486
Severity: CRITICAL
Description: Microsoft Internet Explorer 7 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Memory Corruption V ulnerability," a different vulnerability than CVE-2015-2487, CVE-2015-2490, CVE-2015-2492, CVE-2015 -2494, CVE-2015-2498, and CVE-2015-2499.

CVE ID: CVE-2015-2487
Severity: CRITICAL
Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Memory Corruption Vulnerability," a diff erent vulnerability than CVE-2015-2486, CVE-2015-2490, CVE-2015-2492, CVE-2015-2494, CVE-2015 -2498, and CVE-2015-2499.

CVE ID: CVE-2015-2490
Severity: CRITICAL
Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Memory Corruption Vulnerability," a diff erent vulnerability than CVE-2015-2486, CVE-2015-2487, CVE-2015-2492, CVE-2015-2494, CVE-2015 -2498, and CVE-2015-2499.

CVE ID: CVE-2015-2492
Severity: CRITICAL
Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Memory Corruption Vulnerability," a diff erent vulnerability than CVE-2015-2486, CVE-2015-2487, CVE-2015-2490, CVE-2015-2494, CVE-2015 -2498, and CVE-2015-2499.

CVE ID: CVE-2015-2494
Severity: CRITICAL
Description: Microsoft Internet Explorer 7 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Memory Corruption V ulnerability," a different vulnerability than CVE-2015-2486, CVE-2015-2487, CVE-2015-2490, CVE-2015 -2492, CVE-2015-2498, and CVE-2015-2499.

CVE ID: CVE-2015-2498
Severity: CRITICAL
Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Memory Corruption Vulnerability," a diff erent vulnerability than CVE-2015-2486, CVE-2015-2487, CVE-2015-2490, CVE-2015-2492, CVE-2015 -2494, and CVE-2015-2499.

CVE ID: CVE-2015-2499
Severity: CRITICAL
Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Memory Corruption Vulnerability," a diff erent vulnerability than CVE-2015-2486, CVE-2015-2487, CVE-2015-2490, CVE-2015-2492, CVE-2015

-2494, and CVE-2015-2498.

CVE ID: CVE-2015-2502
Severity: CRITICAL
Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Memory Corruption Vulnerability," as ex ploited in the wild in August 2015.

CVE ID: CVE-2015-6048
Severity: CRITICAL
Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-6049.

CVE ID: CVE-2015-6049
Severity: CRITICAL
Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-6048.

CVE ID: CVE-2015-6066
Severity: CRITICAL
Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-6070, CVE-2015-6071, CVE-2015-6074, CVE-2015 -6076, and CVE-2015-6087.

CVE ID: CVE-2015-6070
Severity: CRITICAL
Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-6066, CVE-2015-6071, CVE-2015-6074, CVE-2015 -6076, and CVE-2015-6087.

CVE ID: CVE-2015-6071
Severity: CRITICAL
Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-6066, CVE-2015-6070, CVE-2015-6074, CVE-2015 -6076, and CVE-2015-6087.

CVE ID: CVE-2015-6074
Severity: CRITICAL
Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-6066, CVE-2015-6070, CVE-2015-6071, CVE-2015 -6076, and CVE-2015-6087.

CVE ID: CVE-2015-6076
Severity: CRITICAL
Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-6066, CVE-2015-6070, CVE-2015-6071, CVE-2015 -6074, and CVE-2015-6087.

CVE ID: CVE-2015-6087
Severity: CRITICAL
Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-6066, CVE-2015-6070, CVE-2015-6071, CVE-2015 -6074, and CVE-2015-6076.

CVE ID: CVE-2015-6150
Severity: CRITICAL
Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-6154.

CVE ID: CVE-2015-6154

Severity: CRITICAL
Description: Microsoft Internet Explorer 7 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability," a different vulnerability than CVE-2015-6150.

CVE ID: CVE-2015-6161
Severity: MODERATE
Description: Microsoft Internet Explorer 7 through 11 and Microsoft Edge allow remote attackers to bypass the ASLR protection mechanism via a crafted web site, aka "Microsoft Browser ASLR Bypass."

CVE ID: CVE-2015-6184
Severity: CRITICAL
Description: The CAttrArray object implementation in Microsoft Internet Explorer 7 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (type confusion and memory corruption) via a malformed Cascading Style Sheets (CSS) token sequence in conjunction with modifications to HTML elements, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-6048 and CVE-2015-6049.

CVE ID: CVE-2013-3912
Severity: CRITICAL
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2013-3916.

CVE ID: CVE-2013-3916
Severity: CRITICAL
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2013-3912.

CVE ID: CVE-2014-0268
Severity: MODERATE
Description: Microsoft Internet Explorer 8 through 11 does not properly restrict file installation and registry-key creation, which allows remote attackers to bypass the Mandatory Integrity Control protection mechanism via a crafted web site, aka "Internet Explorer Elevation of Privilege Vulnerability."

CVE ID: CVE-2014-0281
Severity: CRITICAL
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-0287.

CVE ID: CVE-2014-0287
Severity: CRITICAL
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-0281.

CVE ID: CVE-2014-0297
Severity: CRITICAL
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-0308, CVE-2014-0312, and CVE-2014-0324.

CVE ID: CVE-2014-0308
Severity: CRITICAL
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-0297, CVE-2014-0312, and CVE-2014-0324.

CVE ID: CVE-2014-0312
Severity: CRITICAL
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-0297, CVE-2014-0308, and CVE-2014-0324.

CVE ID: CVE-2014-0324
Severity: CRITICAL

Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-0297, CVE-2014-0308, and CVE-2014-0312.

CVE ID: CVE-2014-1778
Severity: IMPORTANT
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary web script with inc reased privileges via unspecified vectors, aka "Internet Explorer Elevation of Privilege Vulnerability," a di fferent vulnerability than CVE-2014-2777.

CVE ID: CVE-2014-1800
Severity: CRITICAL
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability."

CVE ID: CVE-2014-2777
Severity: IMPORTANT
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary web script with inc reased privileges via unspecified vectors, aka "Internet Explorer Elevation of Privilege Vulnerability," a di fferent vulnerability than CVE-2014-1778.

CVE ID: CVE-2014-2784
Severity: CRITICAL
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-4051.

CVE ID: CVE-2014-2789
Severity: CRITICAL
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-2795, CVE-2014-2798, and CVE-2014-2804.

CVE ID: CVE-2014-2795
Severity: CRITICAL
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-2789, CVE-2014-2798, and CVE-2014-2804.

CVE ID: CVE-2014-2798
Severity: CRITICAL
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-2789, CVE-2014-2795, and CVE-2014-2804.

CVE ID: CVE-2014-2804
Severity: CRITICAL
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-2789, CVE-2014-2795, and CVE-2014-2798.

CVE ID: CVE-2014-4051
Severity: CRITICAL
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-2784.

CVE ID: CVE-2014-4092
Severity: CRITICAL
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-4098.

CVE ID: CVE-2014-4098
Severity: CRITICAL
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V

ulnerability," a different vulnerability than CVE-2014-4092.

CVE ID: CVE-2014-4140
Severity: MODERATE
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to bypass the ASLR protection mecha nism via a crafted web site, aka "Internet Explorer ASLR Bypass Vulnerability."

CVE ID: CVE-2014-4141
Severity: CRITICAL
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability."

CVE ID: CVE-2014-6328
Severity: MODERATE
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to bypass the XSS filter via a crafted a ttribute of an element in an HTML document, aka "Internet Explorer XSS Filter Bypass Vulnerability," a d ifferent vulnerability than CVE-2014-6365.

CVE ID: CVE-2014-6346
Severity: MODERATE
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to read content from a different (1) do main or (2) zone via a crafted web site, aka "Internet Explorer Cross-domain Information Disclosure Vul nerability."

CVE ID: CVE-2014-6351
Severity: CRITICAL
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability."

CVE ID: CVE-2014-6365
Severity: MODERATE
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to bypass the XSS filter via a crafted a ttribute of an element in an HTML document, aka "Internet Explorer XSS Filter Bypass Vulnerability," a d ifferent vulnerability than CVE-2014-6328.

CVE ID: CVE-2015-0032
Severity: CRITICAL
Description: vbscript.dll in Microsoft VBScript 5.6 through 5.8, as used with Internet Explorer 8 through 11 and other products, allows remote attackers to execute arbitrary code or cause a denial of service (memory corrup tion) via a crafted web site, aka "VBScript Memory Corruption Vulnerability."

CVE ID: CVE-2015-0043
Severity: CRITICAL
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability."

CVE ID: CVE-2015-1624
Severity: CRITICAL
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability."

CVE ID: CVE-2015-1667
Severity: CRITICAL
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability."

CVE ID: CVE-2015-1684
Severity: MODERATE
Description: VBScript.dll in the Microsoft VBScript 5.6 through 5.8 engine, as used in Internet Explorer 8 through 11 and other products, allows remote attackers to bypass the ASLR protection mechanism via a crafted we b site, aka "VBScript ASLR Bypass."

CVE ID: CVE-2015-1686

Severity: MODERATE
Description: The Microsoft (1) VBScript 5.6 through 5.8 and (2) JScript 5.6 through 5.8 engines, as used in Internet Explorer 8 through 11 and other products, allow remote attackers to bypass the ASLR protection mecha nism via a crafted web site, aka "VBScript and JScript ASLR Bypass."

CVE ID: CVE-2015-2398
Severity: MODERATE
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to bypass the XSS filter via a crafted a ttribute of an element in an HTML document, aka "Internet Explorer XSS Filter Bypass Vulnerability."

CVE ID: CVE-2015-2414
Severity: MODERATE
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to obtain sensitive browsing-history inf ormation via vectors related to image caching, aka "Internet Explorer Information Disclosure Vulnerabilit y."

CVE ID: CVE-2015-2442
Severity: CRITICAL
Description: Microsoft Internet Explorer 8 through 11 and Edge allow remote attackers to execute arbitrary code or c ause a denial of service (memory corruption) via a crafted web site, aka "Memory Corruption Vulnerabilit y," a different vulnerability than CVE-2015-2444.

CVE ID: CVE-2015-2444
Severity: CRITICAL
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Memory Corruption Vulnerability," a diff erent vulnerability than CVE-2015-2442.

CVE ID: CVE-2015-6047
Severity: IMPORTANT
Description: The broker EditWith feature in Microsoft Internet Explorer 8 through 11 allows remote attackers to bypa ss the AppContainer protection mechanism and gain privileges via a DelegateExecute launch of an arbit rary application, as demonstrated by a transition from Low Integrity to Medium Integrity, aka "Internet Ex plorer Elevation of Privilege Vulnerability."

CVE ID: CVE-2015-6052
Severity: MODERATE
Description: The Microsoft (1) VBScript 5.7 and 5.8 and (2) JScript 5.7 and 5.8 engines, as used in Internet Explorer 8 through 11 and other products, allow remote attackers to bypass the ASLR protection mechanism via a crafted web site, aka "VBScript and JScript ASLR Bypass."

CVE ID: CVE-2015-6059
Severity: MODERATE
Description: The Microsoft (1) VBScript 5.7 and 5.8 and (2) JScript 5.7 and 5.8 engines, as used in Internet Explorer 8 through 11 and other products, allow remote attackers to obtain sensitive information from process me mory via a crafted web site, aka "Scripting Engine Information Disclosure Vulnerability."

CVE ID: CVE-2015-6069
Severity: CRITICAL
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-6081.

CVE ID: CVE-2015-6081
Severity: CRITICAL
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-6069.

CVE ID: CVE-2015-6083
Severity: CRITICAL
Description: Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-6151.

CVE ID: CVE-2015-6138
Severity: MODERATE
Description: Microsoft Internet Explorer 8 through 11 mishandles HTML attributes in HTTP responses, which allows

remote attackers to bypass a cross-site scripting (XSS) protection mechanism via unspecified vectors, a ka "Internet Explorer XSS Filter Bypass Vulnerability."

CVE ID: CVE-2015-6144
Severity: MODERATE
Description: Microsoft Internet Explorer 8 through 11 and Microsoft Edge mishandle HTML attributes in HTTP respo nses, which allows remote attackers to bypass a cross-site scripting (XSS) protection mechanism via un specified vectors, aka "Microsoft Browser XSS Filter Bypass Vulnerability."

CVE ID: CVE-2015-6151
Severity: CRITICAL
Description: Microsoft Internet Explorer 8 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Me mory Corruption Vulnerability," a different vulnerability than CVE-2015-6083.

CVE ID: CVE-2013-3914
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability."

CVE ID: CVE-2014-0270
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-0273, CVE-2014-0274, and CVE-2014-0288.

CVE ID: CVE-2014-0273
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-0270, CVE-2014-0274, and CVE-2014-0288.

CVE ID: CVE-2014-0274
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-0270, CVE-2014-0273, and CVE-2014-0288.

CVE ID: CVE-2014-0288
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-0270, CVE-2014-0273, and CVE-2014-0274.

CVE ID: CVE-2014-0293
Severity: MODERATE
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to read content from a different (1) do main or (2) zone via a crafted web site, aka "Internet Explorer Cross-domain Information Disclosure Vul nerability."

CVE ID: CVE-2014-0298
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability."

CVE ID: CVE-2014-1763
Severity: CRITICAL
Description: Use-after-free vulnerability in Microsoft Internet Explorer 9 through 11 allows remote attackers to execut e arbitrary code and bypass a sandbox protection mechanism via unspecified vectors, as demonstrated by VUPEN during a Pwn2Own competition at CanSecWest 2014.

CVE ID: CVE-2014-1773
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-1783, CVE-2014-1784, CVE-2014-1786, CVE-2014

-1795, CVE-2014-1805, CVE-2014-2758, CVE-2014-2759, CVE-2014-2765, CVE-2014-2766, and CVE-

CVE ID: CVE-2014-1783
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-1773, CVE-2014-1784, CVE-2014-1786, CVE-2014 -1795, CVE-2014-1805, CVE-2014-2758, CVE-2014-2759, CVE-2014-2765, CVE-2014-2766, and CVE-

CVE ID: CVE-2014-1784
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-1773, CVE-2014-1783, CVE-2014-1786, CVE-2014 -1795, CVE-2014-1805, CVE-2014-2758, CVE-2014-2759, CVE-2014-2765, CVE-2014-2766, and CVE-

CVE ID: CVE-2014-1786
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-1773, CVE-2014-1783, CVE-2014-1784, CVE-2014 -1795, CVE-2014-1805, CVE-2014-2758, CVE-2014-2759, CVE-2014-2765, CVE-2014-2766, and CVE-

CVE ID: CVE-2014-1795
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-1773, CVE-2014-1783, CVE-2014-1784, CVE-2014 -1786, CVE-2014-1805, CVE-2014-2758, CVE-2014-2759, CVE-2014-2765, CVE-2014-2766, and CVE-

CVE ID: CVE-2014-1805
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-1773, CVE-2014-1783, CVE-2014-1784, CVE-2014 -1786, CVE-2014-1795, CVE-2014-2758, CVE-2014-2759, CVE-2014-2765, CVE-2014-2766, and CVE-

CVE ID: CVE-2014-2758
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-1773, CVE-2014-1783, CVE-2014-1784, CVE-2014 -1786, CVE-2014-1795, CVE-2014-1805, CVE-2014-2759, CVE-2014-2765, CVE-2014-2766, and CVE-

CVE ID: CVE-2014-2759
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-1773, CVE-2014-1783, CVE-2014-1784, CVE-2014 -1786, CVE-2014-1795, CVE-2014-1805, CVE-2014-2758, CVE-2014-2765, CVE-2014-2766, and CVE-

CVE ID: CVE-2014-2765
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-1773, CVE-2014-1783, CVE-2014-1784, CVE-2014 -1786, CVE-2014-1795, CVE-2014-1805, CVE-2014-2758, CVE-2014-2759, CVE-2014-2766, and CVE-

CVE ID: CVE-2014-2766
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-1773, CVE-2014-1783, CVE-2014-1784, CVE-2014 -1786, CVE-2014-1795, CVE-2014-1805, CVE-2014-2758, CVE-2014-2759, CVE-2014-2765, and CVE-

CVE ID: CVE-2014-2775
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d

enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-1773, CVE-2014-1783, CVE-2014-1784, CVE-2014 -1786, CVE-2014-1795, CVE-2014-1805, CVE-2014-2758, CVE-2014-2759, CVE-2014-2765, and CVE-

CVE ID: CVE-2014-2782
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-1773, CVE-2014-1783, CVE-2014-1784, CVE-2014 -1786, CVE-2014-1795, CVE-2014-1805, CVE-2014-2758, CVE-2014-2759, CVE-2014-2765, CVE-201 4-2766, and CVE-2014-2775.

CVE ID: CVE-2014-2786
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-2792 and CVE-2014-2813.

CVE ID: CVE-2014-2792
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-2786 and CVE-2014-2813.

CVE ID: CVE-2014-2813
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2014-2786 and CVE-2014-2792.

CVE ID: CVE-2014-4058
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability."

CVE ID: CVE-2014-4099
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability."

CVE ID: CVE-2014-6343
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability."

CVE ID: CVE-2014-6369
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability."

CVE ID: CVE-2015-0038
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-0042 and CVE-2015-0046.

CVE ID: CVE-2015-0042
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-0038 and CVE-2015-0046.

CVE ID: CVE-2015-0046
Severity: CRITICAL

Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-0038 and CVE-2015-0042.

CVE ID: CVE-2015-0071
Severity: MODERATE
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to bypass the ASLR protection mechanism via a crafted web site, aka "Internet Explorer ASLR Bypass Vulnerability."

CVE ID: CVE-2015-0072
Severity: MODERATE
Description: Cross-site scripting (XSS) vulnerability in Microsoft Internet Explorer 9 through 11 allows remote attackers to bypass the Same Origin Policy and inject arbitrary web script or HTML via vectors involving an IFRAME element that triggers a redirect, a second IFRAME element that does not trigger a redirect, and an eval of a WindowProxy object, aka "Universal XSS (UXSS)."

CVE ID: CVE-2015-1657
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability."

CVE ID: CVE-2015-1689
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1705.

CVE ID: CVE-2015-1705
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1689.

CVE ID: CVE-2015-1729
Severity: MODERATE
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to read content from a different (1) domain or (2) zone via a crafted web site, aka "Internet Explorer Information Disclosure Vulnerability."

CVE ID: CVE-2015-1741
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1752.

CVE ID: CVE-2015-1752
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1741.

CVE ID: CVE-2015-1765
Severity: MODERATE
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to read the browser history via a crafted web site.

CVE ID: CVE-2015-1767
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-2401 and CVE-2015-2408.

CVE ID: CVE-2015-2401
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1767 and CVE-2015-2408.

CVE ID: CVE-2015-2408

Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-1767 and CVE-2015-2401.

CVE ID: CVE-2015-2450
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Memory Corruption Vulnerability," a diff erent vulnerability than CVE-2015-2451.

CVE ID: CVE-2015-2451
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Memory Corruption Vulnerability," a diff erent vulnerability than CVE-2015-2450.

CVE ID: CVE-2015-2485
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Memory Corruption V ulnerability," a different vulnerability than CVE-2015-2491 and CVE-2015-2541.

CVE ID: CVE-2015-2491
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Memory Corruption Vulnerability," a diff erent vulnerability than CVE-2015-2485 and CVE-2015-2541.

CVE ID: CVE-2015-2541
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Memory Corruption Vulnerability," a diff erent vulnerability than CVE-2015-2485 and CVE-2015-2491.

CVE ID: CVE-2015-6046
Severity: MODERATE
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to obtain sensitive information from pr ocess memory via a crafted web site, aka "Internet Explorer Information Disclosure Vulnerability."

CVE ID: CVE-2015-6065
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-6078.

CVE ID: CVE-2015-6078
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Me mory Corruption Vulnerability," a different vulnerability than CVE-2015-6065.

CVE ID: CVE-2015-6086
Severity: MODERATE
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to obtain sensitive information from pr ocess memory via a crafted web site, aka "Internet Explorer Information Disclosure Vulnerability."

CVE ID: CVE-2015-6088
Severity: MODERATE
Description: Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to bypass the ASL R protection mechanism via a crafted web site, aka "Microsoft Browser ASLR Bypass."

CVE ID: CVE-2015-6148
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Me mory Corruption Vulnerability," a different vulnerability than CVE-2015-6156.

CVE ID: CVE-2015-6156

Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2015-6148.

CVE ID: CVE-2015-6164
Severity: IMPORTANT
Description: Microsoft Internet Explorer 9 through 11 improperly implements a cross-site scripting (XSS) protection mechanism, which allows remote attackers to bypass the Same Origin Policy via a crafted web site, aka "Internet Explorer XSS Filter Bypass Vulnerability."

CVE ID: CVE-2016-0005
Severity: MODERATE
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to bypass the Same Origin Policy via u nspecified vectors, aka "Internet Explorer Elevation of Privilege Vulnerability."

CVE ID: CVE-2016-0059
Severity: MODERATE
Description: The Hyperlink Object Library in Microsoft Internet Explorer 9 through 11 allows remote attackers to obta in sensitive information from process memory via a crafted URL in a (1) e-mail message or (2) Office do cument, aka "Internet Explorer Information Disclosure Vulnerability."

CVE ID: CVE-2016-0060
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Me mory Corruption Vulnerability," a different vulnerability than CVE-2016-0061, CVE-2016-0063, CVE-201 6-0067, and CVE-2016-0072.

CVE ID: CVE-2016-0061
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Me mory Corruption Vulnerability," a different vulnerability than CVE-2016-0060, CVE-2016-0063, CVE-201 6-0067, and CVE-2016-0072.

CVE ID: CVE-2016-0063
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2016-0060, CVE-2016-0061, CVE-2016-0067, and CVE-2016-0072.

CVE ID: CVE-2016-0067
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2016-0060, CVE-2016-0061, CVE-2016-0063, and CVE-2016-0072.

CVE ID: CVE-2016-0068
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to bypass the Same Origin Policy via u nspecified vectors, aka "Internet Explorer Elevation of Privilege Vulnerability," a different vulnerability th an CVE-2016-0069.

CVE ID: CVE-2016-0069
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to bypass the Same Origin Policy via u nspecified vectors, aka "Internet Explorer Elevation of Privilege Vulnerability," a different vulnerability th an CVE-2016-0068.

CVE ID: CVE-2016-0072
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2016-0060, CVE-2016-0061, CVE-2016-0063, and CVE-2016-0067.

CVE ID: CVE-2016-0077
Severity: MODERATE
Description: Microsoft Internet Explorer 9 through 11 and Microsoft Edge misparse HTTP responses, which allows r emote attackers to spoof web sites via a crafted URL, aka "Microsoft Browser Spoofing Vulnerability."

CVE ID: CVE-2016-0105
Severity: IMPORTANT
Description: Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Me mory Corruption Vulnerability," a different vulnerability than CVE-2016-0107, CVE-2016-0111, CVE-201 6-0112, and CVE-2016-0113.

CVE ID: CVE-2016-0107
Severity: IMPORTANT
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2016-0105, CVE-2016-0111, CVE-2016-0112, and CVE-2016-0113.

CVE ID: CVE-2016-0111
Severity: IMPORTANT
Description: Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Me mory Corruption Vulnerability," a different vulnerability than CVE-2016-0105, CVE-2016-0107, CVE-201 6-0112, and CVE-2016-0113.

CVE ID: CVE-2016-0112
Severity: IMPORTANT
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2016-0105, CVE-2016-0107, CVE-2016-0111, and CVE-2016-0113.

CVE ID: CVE-2016-0113
Severity: IMPORTANT
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2016-0105, CVE-2016-0107, CVE-2016-0111, and CVE-2016-0112.

CVE ID: CVE-2016-0154
Severity: IMPORTANT
Description: Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Me mory Corruption Vulnerability."

CVE ID: CVE-2016-0162
Severity: MODERATE
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to determine the existence of files via crafted JavaScript code, aka "Internet Explorer Information Disclosure Vulnerability."

CVE ID: CVE-2016-0192
Severity: IMPORTANT
Description: Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Me mory Corruption Vulnerability."

CVE ID: CVE-2016-0199
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2016-0200 and CVE-2016-3211.

CVE ID: CVE-2016-0200
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d

enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2016-0199 and CVE-2016-3211.

CVE ID: CVE-2016-3204
Severity: CRITICAL
Description: The Microsoft (1) JScript 5.8 and 9 and (2) VBScript 5.7 and 5.8 engines, as used in Internet Explorer 9 through 11 and other products, allow remote attackers to execute arbitrary code or cause a denial of ser vice (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability."

CVE ID: CVE-2016-3211
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2016-0199 and CVE-2016-0200.

CVE ID: CVE-2016-3212
Severity: MODERATE
Description: The XSS Filter in Microsoft Internet Explorer 9 through 11 does not properly identify JavaScript, which makes it easier for remote attackers to conduct cross-site scripting (XSS) attacks via a crafted web site, aka "Internet Explorer XSS Filter Vulnerability."

CVE ID: CVE-2016-3213
Severity: CRITICAL
Description: The Web Proxy Auto Discovery (WPAD) protocol implementation in Microsoft Windows Vista SP2, Win dows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2 , Windows RT 8.1, Windows 10 Gold and 1511, and Internet Explorer 9 through 11 has an improper fall back mechanism, which allows remote attackers to gain privileges via NetBIOS name responses, aka " WPAD Elevation of Privilege Vulnerability."

CVE ID: CVE-2016-3240
Severity: IMPORTANT
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2016-3241 and CVE-2016-3242.

CVE ID: CVE-2016-3241
Severity: IMPORTANT
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2016-3240 and CVE-2016-3242.

CVE ID: CVE-2016-3242
Severity: IMPORTANT
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability," a different vulnerability than CVE-2016-3240 and CVE-2016-3241.

CVE ID: CVE-2016-3245
Severity: MODERATE
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to trick users into making TCP connect ions to a restricted port via a crafted web site, aka "Internet Explorer Security Feature Bypass Vulnerabil ity."

CVE ID: CVE-2016-3248
Severity: CRITICAL
Description: The Microsoft (1) JScript 9, (2) VBScript, and (3) Chakra JavaScript engines, as used in Microsoft Inter net Explorer 9 through 11, Microsoft Edge, and other products, allow remote attackers to execute arbitra ry code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine M emory Corruption Vulnerability," a different vulnerability than CVE-2016-3259.

CVE ID: CVE-2016-3259
Severity: CRITICAL
Description: The Microsoft (1) JScript 9, (2) VBScript, and (3) Chakra JavaScript engines, as used in Microsoft Inter net Explorer 9 through 11, Microsoft Edge, and other products, allow remote attackers to execute arbitra ry code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine M emory Corruption Vulnerability," a different vulnerability than CVE-2016-3248.

CVE ID: CVE-2016-3264

Severity: IMPORTANT
Description: Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability."

CVE ID: CVE-2016-3267
Severity: MODERATE
Description: Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to determine the existence of unspecified files via a crafted web site, aka "Microsoft Browser Information Disclosure Vulnerability."

CVE ID: CVE-2016-3273
Severity: LOW
Description: The XSS Filter in Microsoft Internet Explorer 9 through 11 and Microsoft Edge does not properly restrict JavaScript code, which allows remote attackers to obtain sensitive information via a crafted web site, aka "Microsoft Browser Information Disclosure Vulnerability."

CVE ID: CVE-2016-3274
Severity: LOW
Description: Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to conduct content-spoofing attacks via a crafted URL, aka "Microsoft Browser Spoofing Vulnerability."

CVE ID: CVE-2016-3293
Severity: IMPORTANT
Description: Microsoft Internet Explorer 9 through 11 and Edge allow remote attackers to execute arbitrary code via a crafted web page, aka "Microsoft Browser Memory Corruption Vulnerability."

CVE ID: CVE-2016-3297
Severity: IMPORTANT
Description: Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability."

CVE ID: CVE-2016-3298
Severity: LOW
Description: Microsoft Internet Explorer 9 through 11 and the Internet Messaging API in Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allow remote attackers to determine the existence of arbitrary files via a crafted web site, aka "Internet Explorer Information Disclosure Vulnerability."

CVE ID: CVE-2016-3324
Severity: IMPORTANT
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability."

CVE ID: CVE-2016-3326
Severity: LOW
Description: Microsoft Internet Explorer 9 through 11 and Edge allow remote attackers to obtain sensitive information via a crafted web page, aka "Microsoft Browser Information Disclosure Vulnerability," a different vulnerability than CVE-2016-3327.

CVE ID: CVE-2016-3327
Severity: LOW
Description: Microsoft Internet Explorer 9 through 11 and Edge allow remote attackers to obtain sensitive information via a crafted web page, aka "Microsoft Browser Information Disclosure Vulnerability," a different vulnerability than CVE-2016-3326.

CVE ID: CVE-2016-3329
Severity: LOW
Description: Microsoft Internet Explorer 9 through 11 and Edge allow remote attackers to determine the existence of files via a crafted webpage, aka "Internet Explorer Information Disclosure Vulnerability."

CVE ID: CVE-2016-3351
Severity: LOW
Description: Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to obtain sensitive information via a crafted web site, aka "Microsoft Browser Information Disclosure Vulnerability."

CVE ID: CVE-2016-3353

Severity: MODERATE
Description: Microsoft Internet Explorer 9 through 11 mishandles .url files from the Internet zone, which allows remot e attackers to bypass intended access restrictions via a crafted file, aka "Internet Explorer Security Feat ure Bypass."

CVE ID: CVE-2016-3375
Severity: IMPORTANT
Description: The OLE Automation mechanism and VBScript scripting engine in Microsoft Internet Explorer 9 through 11, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windo ws Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allow remote att ackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability."

CVE ID: CVE-2016-3382
Severity: CRITICAL
Description: The scripting engines in Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attac kers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a s demonstrated by the Chakra JavaScript engine, aka "Scripting Engine Memory Corruption Vulnerabilit

CVE ID: CVE-2016-3384
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a d enial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption V ulnerability."

CVE ID: CVE-2016-3385
Severity: CRITICAL
Description: The scripting engine in Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbi trary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability."

CVE ID: CVE-2016-7195
Severity: IMPORTANT
Description: Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Me mory Corruption Vulnerability," a different vulnerability than CVE-2016-7198.

CVE ID: CVE-2016-7198
Severity: IMPORTANT
Description: Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Me mory Corruption Vulnerability," a different vulnerability than CVE-2016-7195.

CVE ID: CVE-2016-7199
Severity: LOW
Description: Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to bypass the Sam e Origin Policy and obtain sensitive window-state information via a crafted web site, aka "Microsoft Brow ser Information Disclosure Vulnerability."

CVE ID: CVE-2016-7227
Severity: LOW
Description: The scripting engines in Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attac kers to determine the existence of local files via unspecified vectors, aka "Microsoft Browser Information Disclosure Vulnerability."

CVE ID: CVE-2016-7239
Severity: LOW
Description: The RegEx class in the XSS filter in Microsoft Internet Explorer 9 through 11 and Microsoft Edge allows remote attackers to conduct cross-site scripting (XSS) attacks and obtain sensitive information via unsp ecified vectors, aka "Microsoft Browser Information Disclosure Vulnerability."

CVE ID: CVE-2016-7278
Severity: LOW
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to obtain sensitive information from pr ocess memory via a crafted web site, aka "Windows Hyperlink Object Library Information Disclosure Vul nerability."

CVE ID: CVE-2016-7279

Severity: IMPORTANT
Description: Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability."

CVE ID: CVE-2016-7282
Severity: MODERATE
Description: Cross-site scripting (XSS) vulnerability in Microsoft Internet Explorer 9 through 11 and Microsoft Edge allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, aka "Microsoft Browser Information Disclosure Vulnerability."

CVE ID: CVE-2016-7283
Severity: CRITICAL
Description: Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability."

CVE ID: CVE-2013-5045
Severity: IMPORTANT
Description: Microsoft Internet Explorer 10 and 11 allows local users to bypass the Protected Mode protection mechanism, and consequently gain privileges, by leveraging the ability to execute sandboxed code, aka "Internet Explorer Elevation of Privilege Vulnerability."

CVE ID: CVE-2013-5051
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability."

CVE ID: CVE-2014-0313
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-0321.

CVE ID: CVE-2014-0321
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-0313.

CVE ID: CVE-2014-1777
Severity: MODERATE
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to read local files on the client via a crafted web site, aka "Internet Explorer Information Disclosure Vulnerability."

CVE ID: CVE-2014-1780
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-1772, CVE-2014-1794, CVE-2014-1797, CVE-2014-1802, CVE-2014-2756, CVE-2014-2763, CVE-2014-2764, CVE-2014-2769, and CVE-2014-2771.

CVE ID: CVE-2014-1794
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-1772, CVE-2014-1780, CVE-2014-1797, CVE-2014-1802, CVE-2014-2756, CVE-2014-2763, CVE-2014-2764, CVE-2014-2769, and CVE-2014-2771.

CVE ID: CVE-2014-1797
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-1772, CVE-2014-1780, CVE-2014-1794, CVE-2014-1802, CVE-2014-2756, CVE-2014-2763, CVE-2014-2764, CVE-2014-2769, and CVE-2014-2771.

CVE ID: CVE-2014-1802

Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-1772, CVE-2014-1780, CVE-2014-1794, CVE-2014-1797, CVE-2014-2756, CVE-2014-2763, CVE-2014-2764, CVE-2014-2769, and CVE-2014-2771.

CVE ID: CVE-2014-2756
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-1772, CVE-2014-1780, CVE-2014-1794, CVE-2014-1797, CVE-2014-1802, CVE-2014-2763, CVE-2014-2764, CVE-2014-2769, and CVE-2014-2771.

CVE ID: CVE-2014-2763
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-1772, CVE-2014-1780, CVE-2014-1794, CVE-2014-1797, CVE-2014-1802, CVE-2014-2756, CVE-2014-2764, CVE-2014-2769, and CVE-2014-2771.

CVE ID: CVE-2014-2764
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-1772, CVE-2014-1780, CVE-2014-1794, CVE-2014-1797, CVE-2014-1802, CVE-2014-2756, CVE-2014-2763, CVE-2014-2769, and CVE-2014-2771.

CVE ID: CVE-2014-2769
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-1772, CVE-2014-1780, CVE-2014-1794, CVE-2014-1797, CVE-2014-1802, CVE-2014-2756, CVE-2014-2763, CVE-2014-2764, and CVE-2014-2771.

CVE ID: CVE-2014-2771
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-1772, CVE-2014-1780, CVE-2014-1794, CVE-2014-1797, CVE-2014-1802, CVE-2014-2756, CVE-2014-2763, CVE-2014-2764, and CVE-2014-2769.

CVE ID: CVE-2014-2796
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-2808, CVE-2014-2825, CVE-2014-4050, CVE-2014-4055, and CVE-2014-4067.

CVE ID: CVE-2014-2801
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability."

CVE ID: CVE-2014-2808
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-2796, CVE-2014-2825, CVE-2014-4050, CVE-2014-4055, and CVE-2014-4067.

CVE ID: CVE-2014-2825
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-2796, CVE-2014-2808, CVE-2014-4050, CVE-2014-4055, and CVE-2014-4067.

CVE ID: CVE-2014-4050

Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-2796, CVE-2014-2808, CVE-2014-2825, CVE-2014-4055, and CVE-2014-4067.

CVE ID: CVE-2014-4055
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-2796, CVE-2014-2808, CVE-2014-2825, CVE-2014-4050, and CVE-2014-4067.

CVE ID: CVE-2014-4067
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-2796, CVE-2014-2808, CVE-2014-2825, CVE-2014-4050, and CVE-2014-4055.

CVE ID: CVE-2014-4080
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-4089, CVE-2014-4091, and CVE-2014-4102.

CVE ID: CVE-2014-4089
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-4080, CVE-2014-4091, and CVE-2014-4102.

CVE ID: CVE-2014-4091
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-4080, CVE-2014-4089, and CVE-2014-4102.

CVE ID: CVE-2014-4102
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-4080, CVE-2014-4089, and CVE-2014-4091.

CVE ID: CVE-2014-4126
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability."

CVE ID: CVE-2014-6337
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability."

CVE ID: CVE-2014-6349
Severity: MODERATE
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to gain privileges via a crafted web site, aka "Internet Explorer Elevation of Privilege Vulnerability," a different vulnerability than CVE-2014-6350.

CVE ID: CVE-2014-6350
Severity: MODERATE
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to gain privileges via a crafted web site, aka "Internet Explorer Elevation of Privilege Vulnerability," a different vulnerability than CVE-2014-6349.

CVE ID: CVE-2015-0027
Severity: CRITICAL

Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-0035, CVE-2015-0039, CVE-2015-0052, and CVE-2015-0068.

CVE ID: CVE-2015-0035
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-0027, CVE-2015-0039, CVE-2015-0052, and CVE-2015-0068.

CVE ID: CVE-2015-0039
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-0027, CVE-2015-0035, CVE-2015-0052, and CVE-2015-0068.

CVE ID: CVE-2015-0052
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-0027, CVE-2015-0035, CVE-2015-0039, and CVE-2015-0068.

CVE ID: CVE-2015-0054
Severity: MODERATE
Description: Microsoft Internet Explorer 7 through 11 allows remote attackers to gain privileges via a crafted web site, aka "Internet Explorer Elevation of Privilege Vulnerability."

CVE ID: CVE-2015-0055
Severity: MODERATE
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to gain privileges via a crafted web site, aka "Internet Explorer Elevation of Privilege Vulnerability."

CVE ID: CVE-2015-0068
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-0027, CVE-2015-0035, CVE-2015-0039, and CVE-2015-0052.

CVE ID: CVE-2015-0069
Severity: MODERATE
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to bypass the ASLR protection mechanism via a crafted web site, aka "Internet Explorer ASLR Bypass Vulnerability."

CVE ID: CVE-2015-1622
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability."

CVE ID: CVE-2015-1668
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability."

CVE ID: CVE-2015-1714
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability."

CVE ID: CVE-2015-1731
Severity: CRITICAL

Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1736, CVE-2015-1737, and CVE-2015-1755.

CVE ID: CVE-2015-1733
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-2389 and CVE-2015-2411.

CVE ID: CVE-2015-1736
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1731, CVE-2015-1737, and CVE-2015-1755.

CVE ID: CVE-2015-1737
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1731, CVE-2015-1736, and CVE-2015-1755.

CVE ID: CVE-2015-1739
Severity: IMPORTANT
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to gain privileges via a crafted web site, aka "Internet Explorer Elevation of Privilege Vulnerability."

CVE ID: CVE-2015-1755
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1731, CVE-2015-1736, and CVE-2015-1737.

CVE ID: CVE-2015-2389
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1733 and CVE-2015-2411.

CVE ID: CVE-2015-2411
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1733 and CVE-2015-2389.

CVE ID: CVE-2015-2412
Severity: MODERATE
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to read arbitrary local files via a crafted pathname, aka "Internet Explorer Information Disclosure Vulnerability."

CVE ID: CVE-2015-2419
Severity: CRITICAL
Description: JScript 9 in Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "JScript9 Memory Corruption Vulnerability."

CVE ID: CVE-2015-2443
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Memory Corruption Vulnerability."

CVE ID: CVE-2015-2483
Severity: MODERATE
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka "Information Disclosure Vulnerability."

CVE ID: CVE-2015-2484
Severity: IMPORTANT

Description: Microsoft Internet Explorer 10 and 11 uses an incorrect flag during certain filesystem accesses, which a llows remote attackers to delete arbitrary files via unspecified vectors, aka "Tampering Vulnerability."

CVE ID: CVE-2015-2542
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 and Microsoft Edge allow remote attackers to execute arbitrary co de or cause a denial of service (memory corruption) via a crafted web site, aka "Memory Corruption Vul nerability."

CVE ID: CVE-2015-6051
Severity: MODERATE
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to gain privileges via a crafted web site, a s demonstrated by a transition from Low Integrity to Medium Integrity, aka "Internet Explorer Elevation of Privilege Vulnerability."

CVE ID: CVE-2015-6064
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 and Microsoft Edge allow remote attackers to execute arbitrary co de or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Mem ory Corruption Vulnerability," a different vulnerability than CVE-2015-6084 and CVE-2015-6085.

CVE ID: CVE-2015-6084
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a deni al of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vuln erability," a different vulnerability than CVE-2015-6064 and CVE-2015-6085.

CVE ID: CVE-2015-6085
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a deni al of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vuln erability," a different vulnerability than CVE-2015-6064 and CVE-2015-6084.

CVE ID: CVE-2015-6155
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 and Microsoft Edge allow remote attackers to execute arbitrary co de or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Mem ory Corruption Vulnerability."

CVE ID: CVE-2016-0041
Severity: IMPORTANT
Description: Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold and 1511, and Internet Explore r 10 and 11 mishandle DLL loading, which allows local users to gain privileges via a crafted application, aka "DLL Loading Remote Code Execution Vulnerability."

CVE ID: CVE-2016-0110
Severity: IMPORTANT
Description: Microsoft Internet Explorer 10 through 11 and Microsoft Edge allow remote attackers to execute arbitrar y code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability."

CVE ID: CVE-2016-0164
Severity: IMPORTANT
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a deni al of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vuln erability."

CVE ID: CVE-2016-0194
Severity: LOW
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to bypass file permissions and obtain sen sitive information via a crafted web site, aka "Internet Explorer Information Disclosure Vulnerability."

CVE ID: CVE-2016-1096
Severity: IMPORTANT
Description: Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libra ries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vector s, a different vulnerability than other CVEs listed in MS16-064.

CVE ID: CVE-2016-1097
Severity: IMPORTANT
Description: Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libra ries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vector s, a different vulnerability than other CVEs listed in MS16-064.

CVE ID: CVE-2016-1098
Severity: IMPORTANT
Description: Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libra ries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vector s, a different vulnerability than other CVEs listed in MS16-064.

CVE ID: CVE-2016-1099
Severity: IMPORTANT
Description: Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libra ries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vector s, a different vulnerability than other CVEs listed in MS16-064.

CVE ID: CVE-2016-1100
Severity: IMPORTANT
Description: Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libra ries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vector s, a different vulnerability than other CVEs listed in MS16-064.

CVE ID: CVE-2016-1101
Severity: IMPORTANT
Description: Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libra ries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vector s, a different vulnerability than other CVEs listed in MS16-064.

CVE ID: CVE-2016-1102
Severity: IMPORTANT
Description: Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libra ries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vector s, a different vulnerability than other CVEs listed in MS16-064.

CVE ID: CVE-2016-1103
Severity: IMPORTANT
Description: Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libra ries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vector s, a different vulnerability than other CVEs listed in MS16-064.

CVE ID: CVE-2016-1104
Severity: IMPORTANT
Description: Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libra ries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vector s, a different vulnerability than other CVEs listed in MS16-064.

CVE ID: CVE-2016-1105
Severity: IMPORTANT
Description: Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libra ries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vector s, a different vulnerability than other CVEs listed in MS16-064.

CVE ID: CVE-2016-1106
Severity: IMPORTANT
Description: Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libra ries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vector s, a different vulnerability than other CVEs listed in MS16-064.

CVE ID: CVE-2016-1107
Severity: IMPORTANT
Description: Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libra ries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vector s, a different vulnerability than other CVEs listed in MS16-064.

CVE ID: CVE-2016-1108

Severity: IMPORTANT
Description: Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libra ries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vector s, a different vulnerability than other CVEs listed in MS16-064.

CVE ID: CVE-2016-1109
Severity: IMPORTANT
Description: Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libra ries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vector s, a different vulnerability than other CVEs listed in MS16-064.

CVE ID: CVE-2016-1110
Severity: IMPORTANT
Description: Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libra ries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vector s, a different vulnerability than other CVEs listed in MS16-064.

CVE ID: CVE-2016-3243
Severity: IMPORTANT
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a deni al of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vuln erability."

CVE ID: CVE-2016-3277
Severity: LOW
Description: Microsoft Internet Explorer 10 and 11 and Microsoft Edge allow remote attackers to obtain sensitive info rmation via a crafted web site, aka "Microsoft Browser Information Disclosure Vulnerability."

CVE ID: CVE-2016-3292
Severity: MODERATE
Description: Microsoft Internet Explorer 10 and 11 mishandles integrity settings and zone settings, which allows rem ote attackers to bypass a sandbox protection mechanism via a crafted web site, aka "Internet Explorer E levation of Privilege Vulnerability."

CVE ID: CVE-2016-3295
Severity: MODERATE
Description: Microsoft Internet Explorer 10 and 11 and Microsoft Edge allow remote attackers to execute arbitrary co de or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Mem ory Corruption Vulnerability."

CVE ID: CVE-2016-3321
Severity: LOW
Description: Microsoft Internet Explorer 10 and 11 load different files for attempts to open a file:// URL depending on whether the file exists, which allows local users to enumerate files via vectors involving a file:// URL and an HTML5 sandbox iframe, aka "Internet Explorer Information Disclosure Vulnerability."

CVE ID: CVE-2016-3383
Severity: CRITICAL
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a deni al of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vul nerability."

CVE ID: CVE-2016-3387
Severity: IMPORTANT
Description: Microsoft Internet Explorer 10 and 11 and Microsoft Edge do not properly restrict access to private nam espaces, which allows remote attackers to gain privileges via unspecified vectors, aka "Microsoft Brows er Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-3388.

CVE ID: CVE-2016-3388
Severity: LOW
Description: Microsoft Internet Explorer 10 and 11 and Microsoft Edge do not properly restrict access to private nam espaces, which allows remote attackers to gain privileges via unspecified vectors, aka "Microsoft Brows er Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-3387.

CVE ID: CVE-2016-3391
Severity: LOW
Description: Microsoft Internet Explorer 10 and 11 and Microsoft Edge allow context-dependent attackers to discove r credentials by leveraging access to a memory dump, aka "Microsoft Browser Information Disclosure V

ulnerability."

CVE ID: CVE-2016-4108
Severity: IMPORTANT
Description: Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libra ries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vector s, a different vulnerability than other CVEs listed in MS16-064.

CVE ID: CVE-2016-4109
Severity: IMPORTANT
Description: Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libra ries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vector s, a different vulnerability than other CVEs listed in MS16-064.

CVE ID: CVE-2016-4110
Severity: IMPORTANT
Description: Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libra ries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vector s, a different vulnerability than other CVEs listed in MS16-064.

CVE ID: CVE-2016-4111
Severity: IMPORTANT
Description: Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libra ries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vector s, a different vulnerability than other CVEs listed in MS16-064.

CVE ID: CVE-2016-4112
Severity: IMPORTANT
Description: Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libra ries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vector s, a different vulnerability than other CVEs listed in MS16-064.

CVE ID: CVE-2016-4113
Severity: IMPORTANT
Description: Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libra ries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vector s, a different vulnerability than other CVEs listed in MS16-064.

CVE ID: CVE-2016-4114
Severity: IMPORTANT
Description: Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libra ries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vector s, a different vulnerability than other CVEs listed in MS16-064.

CVE ID: CVE-2016-4115
Severity: IMPORTANT
Description: Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libra ries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vector s, a different vulnerability than other CVEs listed in MS16-064.

CVE ID: CVE-2016-4116
Severity: IMPORTANT
Description: Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libra ries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vector s, a different vulnerability than other CVEs listed in MS16-064.

CVE ID: CVE-2016-7196
Severity: IMPORTANT
Description: Microsoft Internet Explorer 10 and 11 and Microsoft Edge allow remote attackers to execute arbitrary co de or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Mem ory Corruption Vulnerability."

CVE ID: CVE-2016-7281
Severity: LOW
Description: The Web Workers implementation in Microsoft Internet Explorer 10 and 11 and Microsoft Edge allows r emote attackers to bypass the Same Origin Policy via unspecified vectors, aka "Microsoft Browser Secu rity Feature Bypass Vulnerability."

CVE ID: CVE-2016-7284

Severity: MODERATE
Description: Microsoft Internet Explorer 10 and 11 allows remote attackers to obtain sensitive information from proce ss memory via a crafted web site, aka "Internet Explorer Information Disclosure Vulnerability."

CVE ID: CVE-2014-0267
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-0289 and CVE-2014-0290.

CVE ID: CVE-2014-0289
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-0267 and CVE-2014-0290.

CVE ID: CVE-2014-0290
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-0267 and CVE-2014-0289.

CVE ID: CVE-2014-0304
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability. "

CVE ID: CVE-2014-1760
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability. "

CVE ID: CVE-2014-1769
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-1782, CVE-2014-1785, CVE-2014-2753, CVE-2014-2755, CVE -2014-2760, CVE-2014-2761, CVE-2014-2772, and CVE-2014-2776.

CVE ID: CVE-2014-1782
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-1769, CVE-2014-1785, CVE-2014-2753, CVE-2014-2755, CVE -2014-2760, CVE-2014-2761, CVE-2014-2772, and CVE-2014-2776.

CVE ID: CVE-2014-1785
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-1769, CVE-2014-1782, CVE-2014-2753, CVE-2014-2755, CVE -2014-2760, CVE-2014-2761, CVE-2014-2772, and CVE-2014-2776.

CVE ID: CVE-2014-2753
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-1769, CVE-2014-1782, CVE-2014-1785, CVE-2014-2755, CVE -2014-2760, CVE-2014-2761, CVE-2014-2772, and CVE-2014-2776.

CVE ID: CVE-2014-2755
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-1769, CVE-2014-1782, CVE-2014-1785, CVE-2014-2753, CVE -2014-2760, CVE-2014-2761, CVE-2014-2772, and CVE-2014-2776.

CVE ID: CVE-2014-2760
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-1769, CVE-2014-1782, CVE-2014-1785, CVE-2014-2753, CVE -2014-2755, CVE-2014-2761, CVE-2014-2772, and CVE-2014-2776.

CVE ID: CVE-2014-2761
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-1769, CVE-2014-1782, CVE-2014-1785, CVE-2014-2753, CVE -2014-2755, CVE-2014-2760, CVE-2014-2772, and CVE-2014-2776.

CVE ID: CVE-2014-2772
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-1769, CVE-2014-1782, CVE-2014-1785, CVE-2014-2753, CVE -2014-2755, CVE-2014-2760, CVE-2014-2761, and CVE-2014-2776.

CVE ID: CVE-2014-2776
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-1769, CVE-2014-1782, CVE-2014-1785, CVE-2014-2753, CVE -2014-2755, CVE-2014-2760, CVE-2014-2761, and CVE-2014-2772.

CVE ID: CVE-2014-2787
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-2790, CVE-2014-2802, and CVE-2014-2806.

CVE ID: CVE-2014-2790
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-2787, CVE-2014-2802, and CVE-2014-2806.

CVE ID: CVE-2014-2802
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-2787, CVE-2014-2790, and CVE-2014-2806.

CVE ID: CVE-2014-2806
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-2787, CVE-2014-2790, and CVE-2014-2802.

CVE ID: CVE-2014-2810
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-2811, CVE-2014-2822, CVE-2014-2823, and CVE-2014-4057.

CVE ID: CVE-2014-2811
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-2810, CVE-2014-2822, CVE-2014-2823, and CVE-2014-4057.

CVE ID: CVE-2014-2822
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se

rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-2810, CVE-2014-2811, CVE-2014-2823, and CVE-2014-4057.

CVE ID: CVE-2014-2823
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-2810, CVE-2014-2811, CVE-2014-2822, and CVE-2014-4057.

CVE ID: CVE-2014-4057
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-2810, CVE-2014-2811, CVE-2014-2822, and CVE-2014-2823.

CVE ID: CVE-2014-4087
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-4095, CVE-2014-4096, and CVE-2014-4101.

CVE ID: CVE-2014-4095
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-4087, CVE-2014-4096, and CVE-2014-4101.

CVE ID: CVE-2014-4096
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-4087, CVE-2014-4095, and CVE-2014-4101.

CVE ID: CVE-2014-4101
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-4087, CVE-2014-4095, and CVE-2014-4096.

CVE ID: CVE-2014-4130
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-4132 and CVE-2014-4138.

CVE ID: CVE-2014-4132
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-4130 and CVE-2014-4138.

CVE ID: CVE-2014-4138
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-4130 and CVE-2014-4132.

CVE ID: CVE-2014-6327
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-6329 and CVE-2014-6376.

CVE ID: CVE-2014-6329
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-6327 and CVE-2014-6376.

CVE ID: CVE-2014-6347
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability. "

CVE ID: CVE-2014-6368
Severity: MODERATE
Description: Microsoft Internet Explorer 11 allows remote attackers to bypass the ASLR protection mechanism via a crafted web site, aka "Internet Explorer ASLR Bypass Vulnerability."

CVE ID: CVE-2014-6376
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2014-6327 and CVE-2014-6329.

CVE ID: CVE-2015-0018
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2015-0037, CVE-2015-0040, and CVE-2015-0066.

CVE ID: CVE-2015-0037
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2015-0018, CVE-2015-0040, and CVE-2015-0066.

CVE ID: CVE-2015-0040
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2015-0018, CVE-2015-0037, and CVE-2015-0066.

CVE ID: CVE-2015-0056
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2015-1623 and CVE-2015-1626.

CVE ID: CVE-2015-0066
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2015-0018, CVE-2015-0037, and CVE-2015-0040.

CVE ID: CVE-2015-1623
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2015-0056 and CVE-2015-1626.

CVE ID: CVE-2015-1626
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2015-0056 and CVE-2015-1623.

CVE ID: CVE-2015-1658
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2015-1706, CVE-2015-1711, CVE-2015-1717, and CVE-2015-1718.

CVE ID: CVE-2015-1659
Severity: CRITICAL

Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2015-1662 and CVE-2015-1665.

CVE ID: CVE-2015-1662
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2015-1659 and CVE-2015-1665.

CVE ID: CVE-2015-1665
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2015-1659 and CVE-2015-1662.

CVE ID: CVE-2015-1685
Severity: MODERATE
Description: Microsoft Internet Explorer 11 allows remote attackers to bypass the ASLR protection mechanism via a crafted web site, aka "Internet Explorer ASLR Bypass."

CVE ID: CVE-2015-1706
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2015-1658, CVE-2015-1711, CVE-2015-1717, and CVE-2015-1718.

CVE ID: CVE-2015-1711
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2015-1658, CVE-2015-1706, CVE-2015-1717, and CVE-2015-1718.

CVE ID: CVE-2015-1713
Severity: IMPORTANT
Description: Microsoft Internet Explorer 11 allows remote attackers to gain privileges via a crafted web site, aka "Inte rnet Explorer Elevation of Privilege Vulnerability."

CVE ID: CVE-2015-1717
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2015-1658, CVE-2015-1706, CVE-2015-1711, and CVE-2015-1718.

CVE ID: CVE-2015-1718
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2015-1658, CVE-2015-1706, CVE-2015-1711, and CVE-2015-1717.

CVE ID: CVE-2015-1732
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2015-1742, CVE-2015-1747, CVE-2015-1750, and CVE-2015-1753.

CVE ID: CVE-2015-1742
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2015-1732, CVE-2015-1747, CVE-2015-1750, and CVE-2015-1753.

CVE ID: CVE-2015-1747
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2015-1732, CVE-2015-1742, CVE-2015-1750, and CVE-2015-1753.

CVE ID: CVE-2015-1750

Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2015-1732, CVE-2015-1742, CVE-2015-1747, and CVE-2015-1753.

CVE ID: CVE-2015-1753
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2015-1732, CVE-2015-1742, CVE-2015-1747, and CVE-2015-1750.

CVE ID: CVE-2015-2383
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2015-2384 and CVE-2015-2425.

CVE ID: CVE-2015-2384
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2015-2383 and CVE-2015-2425.

CVE ID: CVE-2015-2425
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2015-2383 and CVE-2015-2384.

CVE ID: CVE-2015-2446
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 and Edge allow remote attackers to execute arbitrary code or cause a de nial of service (memory corruption) via a crafted web site, aka "Memory Corruption Vulnerability," a diffe rent vulnerability than CVE-2015-2447.

CVE ID: CVE-2015-2447
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Memory Corruption Vulnerability," a different vuln erability than CVE-2015-2446.

CVE ID: CVE-2015-2489
Severity: MODERATE
Description: Microsoft Internet Explorer 11 allows remote attackers to gain privileges via a crafted web site, as demo nstrated by a transition from Low Integrity to Medium Integrity, aka "Elevation of Privilege Vulnerability."

CVE ID: CVE-2015-6042
Severity: CRITICAL
Description: Use-after-free vulnerability in the CWindow object implementation in Microsoft Internet Explorer 11 allo ws remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a cra fted web site, aka "Internet Explorer Memory Corruption Vulnerability."

CVE ID: CVE-2015-6045
Severity: CRITICAL
Description: Use-after-free vulnerability in the CElement object implementation in Microsoft Internet Explorer 11 allo ws remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via craft ed JavaScript that improperly interacts with use of the Cascading Style Sheets (CSS) empty-cells prope rty for a TABLE element, aka "Internet Explorer Memory Corruption Vulnerability."

CVE ID: CVE-2015-6053
Severity: MODERATE
Description: Microsoft Internet Explorer 11 allows remote attackers to obtain sensitive information from process me mory via crafted parameters in an ArrayBuffer.slice call, aka "Internet Explorer Information Disclosure V ulnerability."

CVE ID: CVE-2015-6068
Severity: CRITICAL

Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2015-6072, CVE-2015-6073, CVE-2015-6075, CVE-2015-6077, CVE -2015-6079, CVE-2015-6080, and CVE-2015-6082.

CVE ID: CVE-2015-6072
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2015-6068, CVE-2015-6073, CVE-2015-6075, CVE-2015-6077, CVE -2015-6079, CVE-2015-6080, and CVE-2015-6082.

CVE ID: CVE-2015-6073
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or c ause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Cor ruption Vulnerability," a different vulnerability than CVE-2015-6068, CVE-2015-6072, CVE-2015-6075, C VE-2015-6077, CVE-2015-6079, CVE-2015-6080, and CVE-2015-6082.

CVE ID: CVE-2015-6075
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2015-6068, CVE-2015-6072, CVE-2015-6073, CVE-2015-6077, CVE -2015-6079, CVE-2015-6080, and CVE-2015-6082.

CVE ID: CVE-2015-6077
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2015-6068, CVE-2015-6072, CVE-2015-6073, CVE-2015-6075, CVE -2015-6079, CVE-2015-6080, and CVE-2015-6082.

CVE ID: CVE-2015-6079
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2015-6068, CVE-2015-6072, CVE-2015-6073, CVE-2015-6075, CVE -2015-6077, CVE-2015-6080, and CVE-2015-6082.

CVE ID: CVE-2015-6080
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2015-6068, CVE-2015-6072, CVE-2015-6073, CVE-2015-6075, CVE -2015-6077, CVE-2015-6079, and CVE-2015-6082.

CVE ID: CVE-2015-6082
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2015-6068, CVE-2015-6072, CVE-2015-6073, CVE-2015-6075, CVE -2015-6077, CVE-2015-6079, and CVE-2015-6080.

CVE ID: CVE-2015-6139
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 and Microsoft Edge mishandle content types, which allows remote attack ers to execute arbitrary web script in a privileged context via a crafted web site, aka "Microsoft Browser Elevation of Privilege Vulnerability."

CVE ID: CVE-2015-6140
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or c ause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Cor ruption Vulnerability," a different vulnerability than CVE-2015-6142, CVE-2015-6143, CVE-2015-6153, C VE-2015-6158, CVE-2015-6159, and CVE-2015-6160.

CVE ID: CVE-2015-6142

Severity: CRITICAL
Description: Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or c ause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Cor ruption Vulnerability," a different vulnerability than CVE-2015-6140, CVE-2015-6143, CVE-2015-6153, C VE-2015-6158, CVE-2015-6159, and CVE-2015-6160.

CVE ID: CVE-2015-6143
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2015-6140, CVE-2015-6142, CVE-2015-6153, CVE-2015-6158, CVE -2015-6159, and CVE-2015-6160.

CVE ID: CVE-2015-6153
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or c ause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Cor ruption Vulnerability," a different vulnerability than CVE-2015-6140, CVE-2015-6142, CVE-2015-6143, C VE-2015-6158, CVE-2015-6159, and CVE-2015-6160.

CVE ID: CVE-2015-6157
Severity: MODERATE
Description: Microsoft Internet Explorer 11 allows remote attackers to obtain sensitive information from process me mory via a crafted web site, aka "Internet Explorer Information Disclosure Vulnerability."

CVE ID: CVE-2015-6158
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or c ause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Cor ruption Vulnerability," a different vulnerability than CVE-2015-6140, CVE-2015-6142, CVE-2015-6143, C VE-2015-6153, CVE-2015-6159, and CVE-2015-6160.

CVE ID: CVE-2015-6159
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or c ause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Cor ruption Vulnerability," a different vulnerability than CVE-2015-6140, CVE-2015-6142, CVE-2015-6143, C VE-2015-6153, CVE-2015-6158, and CVE-2015-6160.

CVE ID: CVE-2015-6160
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2015-6140, CVE-2015-6142, CVE-2015-6143, CVE-2015-6153, CVE -2015-6158, and CVE-2015-6159.

CVE ID: CVE-2016-0062
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or c ause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Cor ruption Vulnerability."

CVE ID: CVE-2016-0102
Severity: IMPORTANT
Description: Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or c ause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Cor ruption Vulnerability," a different vulnerability than CVE-2016-0103, CVE-2016-0106, CVE-2016-0108, C VE-2016-0109, and CVE-2016-0114.

CVE ID: CVE-2016-0103
Severity: IMPORTANT
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2016-0102, CVE-2016-0106, CVE-2016-0108, CVE-2016-0109, and CVE-2016-0114.

CVE ID: CVE-2016-0106
Severity: IMPORTANT

Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2016-0102, CVE-2016-0103, CVE-2016-0108, CVE-2016-0109, and CVE-2016-0114.

CVE ID: CVE-2016-0108
Severity: IMPORTANT
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2016-0102, CVE-2016-0103, CVE-2016-0106, CVE-2016-0109, and CVE-2016-0114.

CVE ID: CVE-2016-0109
Severity: IMPORTANT
Description: Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or c ause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Cor ruption Vulnerability," a different vulnerability than CVE-2016-0102, CVE-2016-0103, CVE-2016-0106, C VE-2016-0108, and CVE-2016-0114.

CVE ID: CVE-2016-0114
Severity: IMPORTANT
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability, " a different vulnerability than CVE-2016-0102, CVE-2016-0103, CVE-2016-0106, CVE-2016-0108, and CVE-2016-0109.

CVE ID: CVE-2016-0160
Severity: IMPORTANT
Description: Microsoft Internet Explorer 11 mishandles DLL loading, which allows local users to gain privileges via a crafted application, aka "DLL Loading Remote Code Execution Vulnerability."

CVE ID: CVE-2016-0166
Severity: IMPORTANT
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of se rvice (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability. "

CVE ID: CVE-2016-0188
Severity: CRITICAL
Description: The User Mode Code Integrity (UMCI) implementation in Device Guard in Microsoft Internet Explorer 1 1 allows remote attackers to bypass a code-signing protection mechanism via unspecified vectors, aka " Internet Explorer Security Feature Bypass."

CVE ID: CVE-2016-3210
Severity: CRITICAL
Description: The Microsoft (1) JScript and (2) VBScript engines, as used in Internet Explorer 11, allow remote attack ers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, ak a "Scripting Engine Memory Corruption Vulnerability."

CVE ID: CVE-2016-3247
Severity: MODERATE
Description: Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or c ause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Cor ruption Vulnerability."

CVE ID: CVE-2016-3260
Severity: CRITICAL
Description: The Microsoft (1) JScript 9, (2) VBScript, and (3) Chakra JavaScript engines, as used in Microsoft Inter net Explorer 11, Microsoft Edge, and other products, allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Cor ruption Vulnerability."

CVE ID: CVE-2016-3261
Severity: LOW
Description: Microsoft Internet Explorer 11 allows remote attackers to obtain sensitive information via a crafted web site, aka "Internet Explorer Information Disclosure Vulnerability."

CVE ID: CVE-2016-3276

Severity: LOW
Description: Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to conduct content-spoofing a ttacks via a crafted URL, aka "Microsoft Browser Spoofing Vulnerability."

CVE ID: CVE-2016-3288
Severity: IMPORTANT
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code via a crafted web page, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3290.

CVE ID: CVE-2016-3289
Severity: IMPORTANT
Description: Microsoft Internet Explorer 11 and Edge allow remote attackers to execute arbitrary code via a crafted web page, aka "Microsoft Browser Memory Corruption Vulnerability," a different vulnerability than CVE-2 016-3322.

CVE ID: CVE-2016-3290
Severity: IMPORTANT
Description: Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code via a crafted web page, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3288.

CVE ID: CVE-2016-3291
Severity: LOW
Description: Microsoft Internet Explorer 11 and Microsoft Edge mishandle cross-origin requests, which allows remot e attackers to obtain sensitive information via a crafted web site, aka "Microsoft Browser Information Dis closure Vulnerability."

CVE ID: CVE-2016-3322
Severity: IMPORTANT
Description: Microsoft Internet Explorer 11 and Edge allow remote attackers to execute arbitrary code via a crafted web page, aka "Microsoft Browser Memory Corruption Vulnerability," a different vulnerability than CVE-2 016-3289.

CVE ID: CVE-2016-3325
Severity: LOW
Description: Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to obtain sensitive information via a crafted web site, aka "Microsoft Browser Information Disclosure Vulnerability."

CVE ID: CVE-2016-3331
Severity: CRITICAL
Description: Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or c ause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Cor ruption Vulnerability."

CVE ID: CVE-2016-3390
Severity: IMPORTANT
Description: The scripting engines in Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to ex ecute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, as demonst rated by the Chakra JavaScript engine, aka "Scripting Engine Memory Corruption Vulnerability."

CVE ID: CVE-2016-7241
Severity: IMPORTANT
Description: Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or c ause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Cor ruption Vulnerability."

CVE ID: CVE-2016-7287
Severity: IMPORTANT
Description: The scripting engines in Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to ex ecute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripti ng Engine Memory Corruption Vulnerability."

CVE ID: CVE-2017-0037
Severity: IMPORTANT
Description: Microsoft Internet Explorer 10 and 11 and Microsoft Edge have a type confusion issue in the Layout::M ultiColumnBoxBuilder::HandleColumnBreakOnColumnSpanningElement function in mshtml.dll, which all ows remote attackers to execute arbitrary code via vectors involving a crafted Cascading Style Sheets (CSS) token sequence and crafted JavaScript code that operates on a TH element.

CVE ID: CVE-2017-0008

Severity: MODERATE
Description: Microsoft Internet Explorer 9 through 11 allow remote attackers to obtain sensitive information from pro cess memory via a crafted web site, aka "Internet Explorer Information Disclosure Vulnerability." This vu lnerability is different from those described in CVE-2017-0009 and CVE-2017-0059.

CVE ID: CVE-2017-0009
Severity: MODERATE
Description: Microsoft Internet Explorer 9 through 11 allow remote attackers to obtain sensitive information from pro cess memory via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability." This vuln erability is different from those described in CVE-2017-0011, CVE-2017-0017, CVE-2017-0065, and CV E-2017-0068.

CVE ID: CVE-2017-0040
Severity: IMPORTANT
Description: The scripting engine in Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbi trary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability." This vulnerability is different from that described in CVE-2017-0130.

CVE ID: CVE-2017-0059
Severity: MODERATE
Description: Microsoft Internet Explorer 9 through 11 allow remote attackers to obtain sensitive information from pro cess memory via a crafted web site, aka "Internet Explorer Information Disclosure Vulnerability." This vu lnerability is different from those described in CVE-2017-0008 and CVE-2017-0009.

CVE ID: CVE-2017-0130
Severity: IMPORTANT
Description: The scripting engine in Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbi trary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability." This vulnerability is different from that described in CVE-2017-0040.

CVE ID: CVE-2017-0149
Severity: IMPORTANT
Description: Microsoft Internet Explorer 9 through 11 allow remote attackers to execute arbitrary code or cause a de nial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vul nerability." This vulnerability is different from those described in CVE-2017-0018 and CVE-2017-0037.

CVE ID: CVE-2017-0018
Severity: IMPORTANT
Description: Microsoft Internet Explorer 10 and 11 allow remote attackers to execute arbitrary code or cause a denia l of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulner ability." This vulnerability is different from those described in CVE-2017-0037 and CVE-2017-0149.

CVE ID: CVE-2017-0012
Severity: MODERATE
Description: Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to spoof web content via a cr afted web site, aka "Microsoft Browser Spoofing Vulnerability." This vulnerability is different from those d escribed in CVE-2017-0033 and CVE-2017-0069.

CVE ID: CVE-2017-0033
Severity: MODERATE
Description: Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to spoof web content via a cr afted web site, aka "Microsoft Browser Spoofing Vulnerability." This vulnerability is different from those d escribed in CVE-2017-0012 and CVE-2017-0069.

CVE ID: CVE-2017-0049
Severity: MODERATE
Description: The VBScript engine in Microsoft Internet Explorer 11 allows remote attackers to obtain sensitive inform ation from process memory via a crafted web site, aka "Scripting Engine Information Disclosure Vulnera bility." This vulnerability is different from those described in CVE-2017-0018, and CVE-2017-0037.

CVE ID: CVE-2017-0154
Severity: MODERATE
Description: Microsoft Internet Explorer 11 on Windows 10, 1511, and 1606 and Windows Server 2016 does not enf orce cross-domain policies, allowing attackers to access information from one domain and inject it into a nother via a crafted application, aka, "Internet Explorer Elevation of Privilege Vulnerability."

CVE ID: CVE-2017-0210

Severity: MODERATE
Description: An elevation of privilege vulnerability exists when Internet Explorer does not properly enforce cross-do main policies, which could allow an attacker to access information from one domain and inject it into ano ther domain, aka "Internet Explorer Elevation of Privilege Vulnerability."

CVE ID: CVE-2017-0202
Severity: IMPORTANT
Description: A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in me mory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary cod e in the context of the current user, a.k.a. "Internet Explorer Memory Corruption Vulnerability."

Adobe Flash Player 17.0.0.188 (update available)

CVE ID: CVE-2015-5122
Severity: CRITICAL
Description: Use-after-free vulnerability in the DisplayObject class in the ActionScript 3 (AS3) implementation in Ado be Flash Player 13.x through 13.0.0.302 on Windows and OS X, 14.x through 18.0.0.203 on Windows a nd OS X, 11.x through 11.2.202.481 on Linux, and 12.x through 18.0.0.204 on Linux Chrome installation s allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted Flash content that leverages improper handling of the opaqueBackground property, as exploited in the wild in July 2015.

CVE ID: CVE-2015-5123
Severity: CRITICAL
Description: Use-after-free vulnerability in the BitmapData class in the ActionScript 3 (AS3) implementation in Adobe Flash Player 13.x through 13.0.0.302 on Windows and OS X, 14.x through 18.0.0.203 on Windows and OS X, 11.x through 11.2.202.481 on Linux, and 12.x through 18.0.0.204 on Linux Chrome installations a llows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via cr afted Flash content that overrides a valueOf function, as exploited in the wild in July 2015.

CVE ID: CVE-2014-0578
Severity: MODERATE
Description: Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, an d Adobe AIR SDK & Compiler before 18.0.0.180 allow remote attackers to bypass the Same Origin Poli cy via unspecified vectors, a different vulnerability than CVE-2015-3115, CVE-2015-3116, CVE-2015-31 25, and CVE-2015-5116.

CVE ID: CVE-2015-3096
Severity: IMPORTANT
Description: Adobe Flash Player before 13.0.0.292 and 14.x through 18.x before 18.0.0.160 on Windows and OS X and before 11.2.202.466 on Linux, Adobe AIR before 18.0.0.144 on Windows and before 18.0.0.143 on OS X and Android, Adobe AIR SDK before 18.0.0.144 on Windows and before 18.0.0.143 on OS X, and Adobe AIR SDK & Compiler before 18.0.0.144 on Windows and before 18.0.0.143 on OS X allow remot e attackers to bypass a CVE-2014-5333 protection mechanism via unspecified vectors.

CVE ID: CVE-2015-3097
Severity: MODERATE
Description: Adobe Flash Player before 13.0.0.292 and 14.x through 18.x before 18.0.0.160, Adobe AIR before 18.0 .0.144, Adobe AIR SDK before 18.0.0.144, and Adobe AIR SDK & Compiler before 18.0.0.144 on 64-bit Windows 7 systems do not properly select a random memory address for the Flash heap, which makes i t easier for attackers to conduct unspecified attacks by predicting this address.

CVE ID: CVE-2015-3098
Severity: MODERATE
Description: Adobe Flash Player before 13.0.0.292 and 14.x through 18.x before 18.0.0.160 on Windows and OS X and before 11.2.202.466 on Linux, Adobe AIR before 18.0.0.144 on Windows and before 18.0.0.143 on OS X and Android, Adobe AIR SDK before 18.0.0.144 on Windows and before 18.0.0.143 on OS X, and Adobe AIR SDK & Compiler before 18.0.0.144 on Windows and before 18.0.0.143 on OS X allow remot e attackers to bypass the Same Origin Policy via unspecified vectors, a different vulnerability than CVE-2015-3099 and CVE-2015-3102.

CVE ID: CVE-2015-3099
Severity: MODERATE
Description: Adobe Flash Player before 13.0.0.292 and 14.x through 18.x before 18.0.0.160 on Windows and OS X and before 11.2.202.466 on Linux, Adobe AIR before 18.0.0.144 on Windows and before 18.0.0.143 on OS X and Android, Adobe AIR SDK before 18.0.0.144 on Windows and before 18.0.0.143 on OS X, and Adobe AIR SDK & Compiler before 18.0.0.144 on Windows and before 18.0.0.143 on OS X allow remot e attackers to bypass the Same Origin Policy via unspecified vectors, a different vulnerability than CVE-2015-3098 and CVE-2015-3102.

CVE ID: CVE-2015-3100
Severity: CRITICAL
Description: Stack-based buffer overflow in Adobe Flash Player before 13.0.0.292 and 14.x through 18.x before 18.0.0.160 on Windows and OS X and before 11.2.202.466 on Linux, Adobe AIR before 18.0.0.144 on Windows and before 18.0.0.143 on OS X and Android, Adobe AIR SDK before 18.0.0.144 on Windows and before 18.0.0.143 on OS X, and Adobe AIR SDK & Compiler before 18.0.0.144 on Windows and before 18.0.0.143 on OS X allows attackers to execute arbitrary code via unspecified vectors.

CVE ID: CVE-2015-3101
Severity: MODERATE
Description: The Flash broker in Adobe Flash Player before 13.0.0.292 and 14.x through 18.x before 18.0.0.160 on Windows and OS X and before 11.2.202.466 on Linux, Adobe AIR before 18.0.0.144 on Windows and before 18.0.0.143 on OS X and Android, Adobe AIR SDK before 18.0.0.144 on Windows and before 18.0.0.143 on OS X, and Adobe AIR SDK & Compiler before 18.0.0.144 on Windows and before 18.0.0.143 on OS X, when Internet Explorer is used, allows attackers to perform a transition from Low Integrity to Medium Integrity via unspecified vectors.

CVE ID: CVE-2015-3102
Severity: MODERATE
Description: Adobe Flash Player before 13.0.0.292 and 14.x through 18.x before 18.0.0.160 on Windows and OS X and before 11.2.202.466 on Linux, Adobe AIR before 18.0.0.144 on Windows and before 18.0.0.143 on OS X and Android, Adobe AIR SDK before 18.0.0.144 on Windows and before 18.0.0.143 on OS X, and Adobe AIR SDK & Compiler before 18.0.0.144 on Windows and before 18.0.0.143 on OS X allow remote attackers to bypass the Same Origin Policy via unspecified vectors, a different vulnerability than CVE-2015-3098 and CVE-2015-3099.

CVE ID: CVE-2015-3103
Severity: CRITICAL
Description: Use-after-free vulnerability in Adobe Flash Player before 13.0.0.292 and 14.x through 18.x before 18.0.0.160 on Windows and OS X and before 11.2.202.466 on Linux, Adobe AIR before 18.0.0.144 on Windows and before 18.0.0.143 on OS X and Android, Adobe AIR SDK before 18.0.0.144 on Windows and before 18.0.0.143 on OS X, and Adobe AIR SDK & Compiler before 18.0.0.144 on Windows and before 18.0.0.143 on OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3106 and CVE-2015-3107.

CVE ID: CVE-2015-3104
Severity: CRITICAL
Description: Integer overflow in Adobe Flash Player before 13.0.0.292 and 14.x through 18.x before 18.0.0.160 on Windows and OS X and before 11.2.202.466 on Linux, Adobe AIR before 18.0.0.144 on Windows and before 18.0.0.143 on OS X and Android, Adobe AIR SDK before 18.0.0.144 on Windows and before 18.0.0.143 on OS X, and Adobe AIR SDK & Compiler before 18.0.0.144 on Windows and before 18.0.0.143 on OS X allows attackers to execute arbitrary code via unspecified vectors.

CVE ID: CVE-2015-3105
Severity: CRITICAL
Description: Adobe Flash Player before 13.0.0.292 and 14.x through 18.x before 18.0.0.160 on Windows and OS X and before 11.2.202.466 on Linux, Adobe AIR before 18.0.0.144 on Windows and before 18.0.0.143 on OS X and Android, Adobe AIR SDK before 18.0.0.144 on Windows and before 18.0.0.143 on OS X, and Adobe AIR SDK & Compiler before 18.0.0.144 on Windows and before 18.0.0.143 on OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.

CVE ID: CVE-2015-3106
Severity: CRITICAL
Description: Use-after-free vulnerability in Adobe Flash Player before 13.0.0.292 and 14.x through 18.x before 18.0.0.160 on Windows and OS X and before 11.2.202.466 on Linux, Adobe AIR before 18.0.0.144 on Windows and before 18.0.0.143 on OS X and Android, Adobe AIR SDK before 18.0.0.144 on Windows and before 18.0.0.143 on OS X, and Adobe AIR SDK & Compiler before 18.0.0.144 on Windows and before 18.0.0.143 on OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3103 and CVE-2015-3107.

CVE ID: CVE-2015-3107
Severity: CRITICAL
Description: Use-after-free vulnerability in Adobe Flash Player before 13.0.0.292 and 14.x through 18.x before 18.0.0.160 on Windows and OS X and before 11.2.202.466 on Linux, Adobe AIR before 18.0.0.144 on Windows and before 18.0.0.143 on OS X and Android, Adobe AIR SDK before 18.0.0.144 on Windows and before 18.0.0.143 on OS X, and Adobe AIR SDK & Compiler before 18.0.0.144 on Windows and before 18.0.0.143 on OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerabi

lity than CVE-2015-3103 and CVE-2015-3106.

CVE ID: CVE-2015-3108
Severity: MODERATE
Description: Adobe Flash Player before 13.0.0.292 and 14.x through 18.x before 18.0.0.160 on Windows and OS X and before 11.2.202.466 on Linux, Adobe AIR before 18.0.0.144 on Windows and before 18.0.0.143 on OS X and Android, Adobe AIR SDK before 18.0.0.144 on Windows and before 18.0.0.143 on OS X, and Adobe AIR SDK & Compiler before 18.0.0.144 on Windows and before 18.0.0.143 on OS X do not properly restrict discovery of memory addresses, which allows attackers to bypass the ASLR protection mechanism via unspecified vectors.

CVE ID: CVE-2015-3113
Severity: CRITICAL
Description: Heap-based buffer overflow in Adobe Flash Player before 13.0.0.296 and 14.x through 18.x before 18.0.0.194 on Windows and OS X and before 11.2.202.468 on Linux allows remote attackers to execute arbitrary code via unspecified vectors, as exploited in the wild in June 2015.

CVE ID: CVE-2015-3114
Severity: MODERATE
Description: Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allow attackers to bypass intended access restrictions and obtain sensitive information via unspecified vectors.

CVE ID: CVE-2015-3115
Severity: MODERATE
Description: Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allow remote attackers to bypass the Same Origin Policy via unspecified vectors, a different vulnerability than CVE-2014-0578, CVE-2015-3116, CVE-2015-3125, and CVE-2015-5116.

CVE ID: CVE-2015-3116
Severity: MODERATE
Description: Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allow remote attackers to bypass the Same Origin Policy via unspecified vectors, a different vulnerability than CVE-2014-0578, CVE-2015-3115, CVE-2015-3125, and CVE-2015-5116.

CVE ID: CVE-2015-3117
Severity: CRITICAL
Description: Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-3123, CVE-2015-3130, CVE-2015-3133, CVE-2015-3134, and CVE-2015-4431.

CVE ID: CVE-2015-3118
Severity: CRITICAL
Description: Use-after-free vulnerability in Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3124, CVE-2015-3127, CVE-2015-3128, CVE-2015-3129, CVE-2015-3131, CVE-2015-3132, CVE-2015-3136, CVE-2015-3137, CVE-2015-4428, CVE-2015-4430, and CVE-2015-5117.

CVE ID: CVE-2015-3119
Severity: CRITICAL
Description: Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2015-3120, CVE-2015-3121, CVE-2015-3122, and CVE-2015-4433.

CVE ID: CVE-2015-3120
Severity: CRITICAL
Description: Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, an

d Adobe AIR SDK & Compiler before 18.0.0.180 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2015-3119, CVE-2015-3121, CVE-20 15-3122, and CVE-2015-4433.

CVE ID: CVE-2015-3121
Severity: CRITICAL
Description: Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, an d Adobe AIR SDK & Compiler before 18.0.0.180 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2015-3119, CVE-2015-3120, CVE-20 15-3122, and CVE-2015-4433.

CVE ID: CVE-2015-3122
Severity: CRITICAL
Description: Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, an d Adobe AIR SDK & Compiler before 18.0.0.180 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2015-3119, CVE-2015-3120, CVE-20 15-3121, and CVE-2015-4433.

CVE ID: CVE-2015-3123
Severity: CRITICAL
Description: Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, an d Adobe AIR SDK & Compiler before 18.0.0.180 allow attackers to execute arbitrary code or cause a de nial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-3117 , CVE-2015-3130, CVE-2015-3133, CVE-2015-3134, and CVE-2015-4431.

CVE ID: CVE-2015-3124
Severity: CRITICAL
Description: Use-after-free vulnerability in Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0. 0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe A IR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allows attackers to execu te arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3118, CVE-2015-3127, CVE-2015-3128, CVE-2015-3129, CVE-2015-3131, CVE-2015-3132, CVE-2015-3136, CVE-2015-3137, CVE-2015-4428, CVE-2015-4430, and CVE-2015-5117.

CVE ID: CVE-2015-3125
Severity: MODERATE
Description: Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, an d Adobe AIR SDK & Compiler before 18.0.0.180 allow remote attackers to bypass the Same Origin Poli cy via unspecified vectors, a different vulnerability than CVE-2014-0578, CVE-2015-3115, CVE-2015-31 16, and CVE-2015-5116.

CVE ID: CVE-2015-3126
Severity: IMPORTANT
Description: Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, an d Adobe AIR SDK & Compiler before 18.0.0.180 allow attackers to cause a denial of service (NULL poin ter dereference) or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2015-4429.

CVE ID: CVE-2015-3127
Severity: CRITICAL
Description: Use-after-free vulnerability in Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0. 0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe A IR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allows attackers to execu te arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3118, CVE-2015-3124, CVE-2015-3128, CVE-2015-3129, CVE-2015-3131, CVE-2015-3132, CVE-2015-3136, CVE-2015-3137, CVE-2015-4428, CVE-2015-4430, and CVE-2015-5117.

CVE ID: CVE-2015-3128
Severity: CRITICAL
Description: Use-after-free vulnerability in Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0. 0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe A IR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allows attackers to execu te arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3118, CVE-2015-3124, CVE-2015-3127, CVE-2015-3129, CVE-2015-3131, CVE-2015-3132, CVE-2015-3136, CVE-2015-3137,

CVE-2015-4428, CVE-2015-4430, and CVE-2015-5117.

CVE ID: CVE-2015-3129
Severity: CRITICAL
Description: Use-after-free vulnerability in Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3118, CVE-2015-3124, CVE-2015-3127, CVE-2015-3128, CVE-2015-3131, CVE-2015-3132, CVE-2015-3136, CVE-2015-3137, CVE-2015-4428, CVE-2015-4430, and CVE-2015-5117.

CVE ID: CVE-2015-3130
Severity: CRITICAL
Description: Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-3117, CVE-2015-3123, CVE-2015-3133, CVE-2015-3134, and CVE-2015-4431.

CVE ID: CVE-2015-3131
Severity: CRITICAL
Description: Use-after-free vulnerability in Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3118, CVE-2015-3124, CVE-2015-3127, CVE-2015-3128, CVE-2015-3129, CVE-2015-3132, CVE-2015-3136, CVE-2015-3137, CVE-2015-4428, CVE-2015-4430, and CVE-2015-5117.

CVE ID: CVE-2015-3132
Severity: CRITICAL
Description: Use-after-free vulnerability in Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3118, CVE-2015-3124, CVE-2015-3127, CVE-2015-3128, CVE-2015-3129, CVE-2015-3131, CVE-2015-3136, CVE-2015-3137, CVE-2015-4428, CVE-2015-4430, and CVE-2015-5117.

CVE ID: CVE-2015-3133
Severity: CRITICAL
Description: Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-3117, CVE-2015-3123, CVE-2015-3130, CVE-2015-3134, and CVE-2015-4431.

CVE ID: CVE-2015-3134
Severity: CRITICAL
Description: Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-3117, CVE-2015-3123, CVE-2015-3130, CVE-2015-3133, and CVE-2015-4431.

CVE ID: CVE-2015-3135
Severity: CRITICAL
Description: Heap-based buffer overflow in Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-4432 and CVE-2015-

CVE ID: CVE-2015-3136
Severity: CRITICAL
Description: Use-after-free vulnerability in Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3118, CVE-2015-3124, CVE-2015-3127, CVE-2015-3128, CVE-2015-3129, CVE-2015-3131, CVE-2015-3132, CVE-2015-3137, CVE-2015-4428, CVE-2015-4430, and CVE-2015-5117.

CVE ID: CVE-2015-3137

Severity: CRITICAL
Description: Use-after-free vulnerability in Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3118, CVE-2015-3124, CVE-2015-3127, CVE-2015-3128, CVE-2015-3129, CVE-2015-3131, CVE-2015-3132, CVE-2015-3136, CVE-2015-4428, CVE-2015-4430, and CVE-2015-5117.

CVE ID: CVE-2015-4428
Severity: CRITICAL
Description: Use-after-free vulnerability in Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3118, CVE-2015-3124, CVE-2015-3127, CVE-2015-3128, CVE-2015-3129, CVE-2015-3131, CVE-2015-3132, CVE-2015-3136, CVE-2015-3137, CVE-2015-4430, and CVE-2015-5117.

CVE ID: CVE-2015-4429
Severity: CRITICAL
Description: Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allow attackers to cause a denial of service (NULL pointer dereference) or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2015-3126.

CVE ID: CVE-2015-4430
Severity: CRITICAL
Description: Use-after-free vulnerability in Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3118, CVE-2015-3124, CVE-2015-3127, CVE-2015-3128, CVE-2015-3129, CVE-2015-3131, CVE-2015-3132, CVE-2015-3136, CVE-2015-3137, CVE-2015-4428, and CVE-2015-5117.

CVE ID: CVE-2015-4431
Severity: CRITICAL
Description: Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-3117, CVE-2015-3123, CVE-2015-3130, CVE-2015-3133, and CVE-2015-3134.

CVE ID: CVE-2015-4432
Severity: CRITICAL
Description: Heap-based buffer overflow in Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3135 and CVE-2015-

CVE ID: CVE-2015-4433
Severity: CRITICAL
Description: Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2015-3119, CVE-2015-3120, CVE-2015-3121, and CVE-2015-3122.

CVE ID: CVE-2015-5116
Severity: MODERATE
Description: Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allow remote attackers to bypass the Same Origin Policy via unspecified vectors, a different vulnerability than CVE-2014-0578, CVE-2015-3115, CVE-2015-3116, and CVE-2015-3125.

CVE ID: CVE-2015-5117
Severity: CRITICAL
Description: Use-after-free vulnerability in Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe A

IR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allows attackers to execu te arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3118, CVE-2015-3124, CVE-2015-3127, CVE-2015-3128, CVE-2015-3129, CVE-2015-3131, CVE-2015-3132, CVE-2015-3136, CVE-2015-3137, CVE-2015-4428, and CVE-2015-4430.

CVE ID: CVE-2015-5118
Severity: CRITICAL
Description: Heap-based buffer overflow in Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0 .0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allows attackers to exec ute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3135 and CVE-2015-

CVE ID: CVE-2015-5119
Severity: CRITICAL
Description: Use-after-free vulnerability in the ByteArray class in the ActionScript 3 (AS3) implementation in Adobe Flash Player 13.x through 13.0.0.296 and 14.x through 18.0.0.194 on Windows and OS X and 11.x thro ugh 11.2.202.468 on Linux allows remote attackers to execute arbitrary code or cause a denial of servic e (memory corruption) via crafted Flash content that overrides a valueOf function, as exploited in the wil d in July 2015.

CVE ID: CVE-2015-5124
Severity: CRITICAL
Description: Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, an d Adobe AIR SDK & Compiler before 18.0.0.180 allow attackers to execute arbitrary code or cause a de nial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-3117 , CVE-2015-3123, CVE-2015-3130, CVE-2015-3133, CVE-2015-3134, and CVE-2015-4431.

CVE ID: CVE-2015-5567
Severity: CRITICAL
Description: Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 1 1.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allow attackers to execute arbitrary code or cause a denial of service (stack memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5579.

CVE ID: CVE-2015-5568
Severity: CRITICAL
Description: Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 1 1.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allow attackers to cause a denial of service (vector-length corruption) or possibly have unspecified other impact via unknown vectors.

CVE ID: CVE-2015-5570
Severity: CRITICAL
Description: Use-after-free vulnerability in Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Win dows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK befor e 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allows attackers to execute arbitrary c ode via unspecified vectors, a different vulnerability than CVE-2015-5574, CVE-2015-5581, CVE-2015-5 584, and CVE-2015-6682.

CVE ID: CVE-2015-5571
Severity: MODERATE
Description: Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 1 1.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 do not properly restrict the SWF file format, which allows remote atta ckers to conduct cross-site request forgery (CSRF) attacks against JSONP endpoints, and obtain sensiti ve information, via a crafted OBJECT element with SWF content satisfying the character-set requiremen ts of a callback API. NOTE: this issue exists because of an incomplete fix for CVE-2014-4671 and CVE -2014-5333.

CVE ID: CVE-2015-5572
Severity: MODERATE
Description: Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 1 1.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allow attackers to bypass intended access restrictions and obtain se nsitive information via unspecified vectors.

CVE ID: CVE-2015-5573

Severity: CRITICAL
Description: Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion."

CVE ID: CVE-2015-5574
Severity: CRITICAL
Description: Use-after-free vulnerability in Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5570, CVE-2015-5581, CVE-2015-5584, and CVE-2015-6682.

CVE ID: CVE-2015-5575
Severity: CRITICAL
Description: Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5577, CVE-2015-5578, CVE-2015-5580, CVE-2015-5582, CVE-2015-5588, and CVE-2015-6677.

CVE ID: CVE-2015-5576
Severity: MODERATE
Description: Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 do not properly restrict discovery of memory addresses, which allows attackers to bypass the ASLR protection mechanism via unspecified vectors.

CVE ID: CVE-2015-5577
Severity: CRITICAL
Description: Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5575, CVE-2015-5578, CVE-2015-5580, CVE-2015-5582, CVE-2015-5588, and CVE-2015-6677.

CVE ID: CVE-2015-5578
Severity: CRITICAL
Description: Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5575, CVE-2015-5577, CVE-2015-5580, CVE-2015-5582, CVE-2015-5588, and CVE-2015-6677.

CVE ID: CVE-2015-5579
Severity: CRITICAL
Description: Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allow attackers to execute arbitrary code or cause a denial of service (stack memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5567.

CVE ID: CVE-2015-5580
Severity: CRITICAL
Description: Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5575, CVE-2015-5577, CVE-2015-5578, CVE-2015-5582, CVE-2015-5588, and CVE-2015-6677.

CVE ID: CVE-2015-5581
Severity: CRITICAL
Description: Use-after-free vulnerability in Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5570, CVE-2015-5574, CVE-2015-5584, and CVE-2015-6682.

CVE ID: CVE-2015-5582

Severity: CRITICAL
Description: Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5575, CVE-2015-5577, CVE-2015-5578, CVE-2015-5580, CVE-2015-5588, and CVE-2015-6677.

CVE ID: CVE-2015-5584
Severity: CRITICAL
Description: Use-after-free vulnerability in Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5570, CVE-2015-5574, CVE-2015-5581, and CVE-2015-6682.

CVE ID: CVE-2015-5587
Severity: CRITICAL
Description: Stack-based buffer overflow in Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allows attackers to execute arbitrary code via unspecified vectors.

CVE ID: CVE-2015-5588
Severity: CRITICAL
Description: Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5575, CVE-2015-5577, CVE-2015-5578, CVE-2015-5580, CVE-2015-5582, and CVE-2015-6677.

CVE ID: CVE-2015-6676
Severity: CRITICAL
Description: Buffer overflow in Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-6678.

CVE ID: CVE-2015-6677
Severity: CRITICAL
Description: Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5575, CVE-2015-5577, CVE-2015-5578, CVE-2015-5580, CVE-2015-5582, and CVE-2015-5588.

CVE ID: CVE-2015-6678
Severity: CRITICAL
Description: Buffer overflow in Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-6676.

CVE ID: CVE-2015-6679
Severity: MODERATE
Description: Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allow attackers to bypass the Same Origin Policy and obtain sensitive information via unspecified vectors.

CVE ID: CVE-2015-6682
Severity: CRITICAL
Description: Use-after-free vulnerability in Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5570, CVE-2015-5574, CVE-2015-5581, and CVE-2015-5584.

WinRAR 4.11.0.0 (update available)
No vulnerabilities found.

Windows Update Agent 7.6.7601.19161 (update available)
No vulnerabilities found.

Windows VPN Client 6.1.7600.16385 (update available)
No vulnerabilities found.

CCleaner 5.04.00.5151 (update available)
No vulnerabilities found.

Microsoft Publisher 12.0.4518.1014 (update available)

CVE ID: CVE-2007-6534
Severity: IMPORTANT
Description: Multiple unspecified vulnerabilities in Microsoft Office Publisher allow user-assisted remote attackers to cause a denial of service (application crash) via a crafted PUB file, possibly involving wordart.

CVE ID: CVE-2008-3068
Severity: IMPORTANT
Description: Microsoft Crypto API 5.131.2600.2180 through 6.0, as used in Outlook, Windows Live Mail, and Office 2007, performs Certificate Revocation List (CRL) checks by using an arbitrary URL from a certificate em bedded in a (1) S/MIME e-mail message or (2) signed document, which allows remote attackers to obtai n reading times and IP addresses of recipients, and port-scan results, via a crafted certificate with an Au thority Information Access (AIA) extension.

CVE ID: CVE-2007-1117
Severity: CRITICAL
Description: Unspecified vulnerability in Publisher 2007 in Microsoft Office 2007 allows remote attackers to execute arbitrary code via unspecified vectors, related to a "file format vulnerability." NOTE: this information is ba sed upon a vague pre-advisory with no actionable information. However, the advisory is from a reliable source.

CVE ID: CVE-2007-1754
Severity: CRITICAL
Description: PUBCONV.DLL in Microsoft Office Publisher 2007 does not properly clear memory when transferring d ata from disk to memory, which allows user-assisted remote attackers to execute arbitrary code via a m alformed .pub page via a certain negative value, which bypasses a sanitization procedure that initializes critical pointers to NULL, aka the "Publisher Invalid Memory Reference Vulnerability".

CVE ID: CVE-2011-1508
Severity: CRITICAL
Description: Microsoft Publisher 2003 SP3, and 2007 SP2 and SP3, does not properly manage memory allocations f or function pointers, which allows user-assisted remote attackers to execute arbitrary code via a crafted Publisher file, aka "Publisher Function Pointer Overwrite Vulnerability."

CVE ID: CVE-2011-3410
Severity: CRITICAL
Description: Array index error in Microsoft Publisher 2003 SP3, and 2007 SP2 and SP3, allows remote attackers to execute arbitrary code via a crafted Publisher file that leverages incorrect handling of values in memory, aka "Publisher Out-of-bounds Array Index Vulnerability."

CVE ID: CVE-2011-3412
Severity: CRITICAL
Description: Microsoft Publisher 2003 SP3, and 2007 SP2 and SP3, allows remote attackers to execute arbitrary co de via a crafted Publisher file that leverages incorrect memory handling, aka "Publisher Memory Corrupt ion Vulnerability."

CVE ID: CVE-2013-1328
Severity: CRITICAL
Description: Microsoft Publisher 2003 SP3, 2007 SP3, and 2010 SP1 allows remote attackers to execute arbitrary c ode via a crafted Publisher file that triggers incorrect pointer handling, aka "Publisher Pointer Handling V ulnerability."

CVE ID: CVE-2014-1759
Severity: CRITICAL
Description: pubconv.dll in Microsoft Publisher 2003 SP3 and 2007 SP3 allows remote attackers to execute arbitrary code or cause a denial of service (incorrect pointer dereference and application crash) via a crafted .pub file, aka "Arbitrary Pointer Dereference Vulnerability."

CVE ID: CVE-2015-2503

Severity: CRITICAL
Description: Microsoft Access 2007 SP3, Excel 2007 SP3, InfoPath 2007 SP3, OneNote 2007 SP3, PowerPoint 200 7 SP3, Project 2007 SP3, Publisher 2007 SP3, Visio 2007 SP3, Word 2007 SP3, Office 2007 IME (Japa nese) SP3, Access 2010 SP2, Excel 2010 SP2, InfoPath 2010 SP2, OneNote 2010 SP2, PowerPoint 20 10 SP2, Project 2010 SP2, Publisher 2010 SP2, Visio 2010 SP2, Word 2010 SP2, Pinyin IME 2010, Acc ess 2013 SP1, Excel 2013 SP1, InfoPath 2013 SP1, OneNote 2013 SP1, PowerPoint 2013 SP1, Project 2013 SP1, Publisher 2013 SP1, Visio 2013 SP1, Word 2013 SP1, Excel 2013 RT SP1, OneNote 2013 RT SP1, PowerPoint 2013 RT SP1, Word 2013 RT SP1, Access 2016, Excel 2016, OneNote 2016, Pow erPoint 2016, Project 2016, Publisher 2016, Visio 2016, Word 2016, Skype for Business 2016, and Lync 2013 SP1 allow remote attackers to bypass a sandbox protection mechanism and gain privileges via a c rafted web site that is accessed with Internet Explorer, as demonstrated by a transition from Low Integrit y to Medium Integrity, aka "Microsoft Office Elevation of Privilege Vulnerability."

Microsoft PowerPoint 12.0.4518.1014 (update available)

CVE ID: CVE-2008-3068
Severity: IMPORTANT
Description: Microsoft Crypto API 5.131.2600.2180 through 6.0, as used in Outlook, Windows Live Mail, and Office 2007, performs Certificate Revocation List (CRL) checks by using an arbitrary URL from a certificate em bedded in a (1) S/MIME e-mail message or (2) signed document, which allows remote attackers to obtai n reading times and IP addresses of recipients, and port-scan results, via a crafted certificate with an Au thority Information Access (AIA) extension.

CVE ID: CVE-2010-3142
Severity: CRITICAL
Description: Untrusted search path vulnerability in Microsoft Office PowerPoint 2007 allows local users, and possibly remote attackers, to execute arbitrary code and conduct DLL hijacking attacks via a Trojan horse rpawin et.dll that is located in the same folder as a .odp, .pothtml, .potm, .potx, .ppa, .ppam, .pps, .ppt, .ppthtml, .pptm, .pptxml, .pwz, .sldm, .sldx, and .thmx file.

CVE ID: CVE-2011-0976
Severity: CRITICAL
Description: Microsoft PowerPoint 2002 SP3, 2003 SP3, and 2007 SP2; Office 2004 and 2008 for Mac; Open XML File Format Converter for Mac; Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File For mats SP2; and PowerPoint Viewer 2007 SP2 do not properly handle Office Art containers that have inva lid records, which allows remote attackers to execute arbitrary code or cause a denial of service (memor y corruption) via a PowerPoint document with a container that triggers certain access to an uninitialized object, aka "OfficeArt Atom RCE Vulnerability."

CVE ID: CVE-2015-0085
Severity: CRITICAL
Description: Use-after-free vulnerability in Microsoft Office 2007 SP3, Excel 2007 SP3, PowerPoint 2007 SP3, Word 2007 SP3, Office 2010 SP2, Excel 2010 SP2, PowerPoint 2010 SP2, Word 2010 SP2, Office 2013 Gold and SP1, Word 2013 Gold and SP1, Office 2013 RT Gold and SP1, Word 2013 RT Gold and SP1, Exce l Viewer, Office Compatibility Pack SP3, Word Automation Services on SharePoint Server 2010 SP2, Ex cel Services on SharePoint Server 2013 Gold and SP1, Word Automation Services on SharePoint Serv er 2013 Gold and SP1, Web Applications 2010 SP2, Office Web Apps Server 2010 SP2, Web Apps Ser ver 2013 Gold and SP1, SharePoint Server 2007 SP3, Windows SharePoint Services 3.0 SP3, SharePo int Foundation 2010 SP2, SharePoint Server 2010 SP2, SharePoint Foundation 2013 Gold and SP1, an d SharePoint Server 2013 Gold and SP1 allows remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Component Use After Free Vulnerability."

CVE ID: CVE-2015-0097
Severity: CRITICAL
Description: Microsoft Excel 2007 SP3, PowerPoint 2007 SP3, Word 2007 SP3, Excel 2010 SP2, PowerPoint 2010 SP2, and Word 2010 SP2 allow remote attackers to execute arbitrary code via a crafted Office documen t, aka "Microsoft Word Local Zone Remote Code Execution Vulnerability."

CVE ID: CVE-2015-2423
Severity: MODERATE
Description: Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, W indows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, Windows 10, Excel 2007 S P3, PowerPoint 2007 SP3, Visio 2007 SP3, Word 2007 SP3, Office 2010 SP2, Excel 2010 SP2, Power Point 2010 SP2, Visio 2010 SP2, Word 2010 SP2, Excel 2013 SP1, PowerPoint 2013 SP1, Visio 2013 SP1, Word 2013 SP1, Excel 2013 RT SP1, PowerPoint 2013 RT SP1, Visio 2013 RT SP1, Word 2013 RT SP1, and Internet Explorer 7 through 11 allow remote attackers to gain privileges and obtain sensitiv e information via a crafted command-line parameter to an Office application or Notepad, as demonstrate d by a transition from Low Integrity to Medium Integrity, aka "Unsafe Command Line Parameter Passing Vulnerability."

CVE ID: CVE-2015-2424
Severity: CRITICAL
Description: Microsoft PowerPoint 2007 SP3, Word 2007 SP3, PowerPoint 2010 SP2, Word 2010 SP2, PowerPoint 2013 SP1, Word 2013 SP1, and PowerPoint 2013 RT SP1 allow remote attackers to execute arbitrary c ode or cause a denial of service (memory corruption) via a crafted Office document, aka "Microsoft Offic e Memory Corruption Vulnerability."

CVE ID: CVE-2015-2503
Severity: CRITICAL
Description: Microsoft Access 2007 SP3, Excel 2007 SP3, InfoPath 2007 SP3, OneNote 2007 SP3, PowerPoint 200 7 SP3, Project 2007 SP3, Publisher 2007 SP3, Visio 2007 SP3, Word 2007 SP3, Office 2007 IME (Japa nese) SP3, Access 2010 SP2, Excel 2010 SP2, InfoPath 2010 SP2, OneNote 2010 SP2, PowerPoint 20 10 SP2, Project 2010 SP2, Publisher 2010 SP2, Visio 2010 SP2, Word 2010 SP2, Pinyin IME 2010, Acc ess 2013 SP1, Excel 2013 SP1, InfoPath 2013 SP1, OneNote 2013 SP1, PowerPoint 2013 SP1, Project 2013 SP1, Publisher 2013 SP1, Visio 2013 SP1, Word 2013 SP1, Excel 2013 RT SP1, OneNote 2013 RT SP1, PowerPoint 2013 RT SP1, Word 2013 RT SP1, Access 2016, Excel 2016, OneNote 2016, Pow erPoint 2016, Project 2016, Publisher 2016, Visio 2016, Word 2016, Skype for Business 2016, and Lync 2013 SP1 allow remote attackers to bypass a sandbox protection mechanism and gain privileges via a c rafted web site that is accessed with Internet Explorer, as demonstrated by a transition from Low Integrit y to Medium Integrity, aka "Microsoft Office Elevation of Privilege Vulnerability."

CVE ID: CVE-2016-3360
Severity: CRITICAL
Description: Microsoft PowerPoint 2007 SP3, PowerPoint 2010 SP2, PowerPoint 2013 SP1, PowerPoint 2013 RT S P1, PowerPoint 2016 for Mac, Office Compatibility Pack SP3, PowerPoint Viewer, SharePoint Server 20 13 SP1, Office Web Apps 2010 SP2, and Office Web Apps Server 2013 SP1 allow remote attackers to execute arbitrary code via a crafted document, aka "Microsoft Office Memory Corruption Vulnerability."

Microsoft Outlook 12.0.4518.1014 (update available)

CVE ID: CVE-2008-3068
Severity: IMPORTANT
Description: Microsoft Crypto API 5.131.2600.2180 through 6.0, as used in Outlook, Windows Live Mail, and Office 2007, performs Certificate Revocation List (CRL) checks by using an arbitrary URL from a certificate em bedded in a (1) S/MIME e-mail message or (2) signed document, which allows remote attackers to obtai n reading times and IP addresses of recipients, and port-scan results, via a crafted certificate with an Au thority Information Access (AIA) extension.

CVE ID: CVE-2013-3870
Severity: CRITICAL
Description: Double free vulnerability in Microsoft Outlook 2007 SP3 and 2010 SP1 and SP2 allows remote attacker s to execute arbitrary code by including many nested S/MIME certificates in an e-mail message, aka "M essage Certificate Vulnerability."

CVE ID: CVE-2013-3905
Severity: MODERATE
Description: Microsoft Outlook 2007 SP3, 2010 SP1 and SP2, 2013, and 2013 RT does not properly expand metada ta contained in S/MIME certificates, which allows remote attackers to obtain sensitive network configurat ion and state information via a crafted certificate in an e-mail message, aka "S/MIME AIA Vulnerability."

CVE ID: CVE-2016-3366
Severity: MODERATE
Description: Microsoft Outlook 2007 SP3, Outlook 2010 SP2, Outlook 2013 SP1, Outlook 2013 RT SP1, Outlook 20 16, and Outlook 2016 for Mac do not properly implement RFC 2046, which allows remote attackers to b ypass virus or spam detection via crafted MIME data in an e-mail attachment, aka "Microsoft Office Spo ofing Vulnerability."

CVE ID: CVE-2017-0106
Severity: CRITICAL
Description: Microsoft Excel 2007 SP3, Microsoft Outlook 2010 SP2, Microsoft Outlook 2013 SP1, and Microsoft Ou tlook 2016 allow remote attackers to execute arbitrary code or cause a denial of service (memory corrup tion) via a crafted document, aka "Microsoft Office Memory Corruption Vulnerability."

CVE ID: CVE-2017-0204
Severity: MODERATE
Description: Microsoft Outlook 2007 SP3, Microsoft Outlook 2010 SP2, Microsoft Outlook 2013 SP1, and Microsoft

Outlook 2016 allow remote attackers to bypass the Office Protected View via a specially crafted docume nt, aka "Microsoft Office Security Feature Bypass Vulnerability."

Microsoft OneNote 12.0.4518.1014 (update available)

CVE ID: CVE-2014-2815
Severity: CRITICAL
Description: Microsoft OneNote 2007 SP3 allows remote attackers to execute arbitrary code via a crafted OneNote f ile that triggers creation of an executable file in a startup folder, aka "OneNote Remote Code Execution Vulnerability."

CVE ID: CVE-2015-2503
Severity: CRITICAL
Description: Microsoft Access 2007 SP3, Excel 2007 SP3, InfoPath 2007 SP3, OneNote 2007 SP3, PowerPoint 200 7 SP3, Project 2007 SP3, Publisher 2007 SP3, Visio 2007 SP3, Word 2007 SP3, Office 2007 IME (Japa nese) SP3, Access 2010 SP2, Excel 2010 SP2, InfoPath 2010 SP2, OneNote 2010 SP2, PowerPoint 20 10 SP2, Project 2010 SP2, Publisher 2010 SP2, Visio 2010 SP2, Word 2010 SP2, Pinyin IME 2010, Acc ess 2013 SP1, Excel 2013 SP1, InfoPath 2013 SP1, OneNote 2013 SP1, PowerPoint 2013 SP1, Project 2013 SP1, Publisher 2013 SP1, Visio 2013 SP1, Word 2013 SP1, Excel 2013 RT SP1, OneNote 2013 RT SP1, PowerPoint 2013 RT SP1, Word 2013 RT SP1, Access 2016, Excel 2016, OneNote 2016, Pow erPoint 2016, Project 2016, Publisher 2016, Visio 2016, Word 2016, Skype for Business 2016, and Lync 2013 SP1 allow remote attackers to bypass a sandbox protection mechanism and gain privileges via a c rafted web site that is accessed with Internet Explorer, as demonstrated by a transition from Low Integrit y to Medium Integrity, aka "Microsoft Office Elevation of Privilege Vulnerability."

CVE ID: CVE-2016-3315
Severity: MODERATE
Description: Microsoft OneNote 2007 SP3, 2010 SP2, 2013 SP1, 2013 RT SP1, 2016, and 2016 for Mac allow remo te attackers to obtain sensitive information via a crafted OneNote file, aka "Microsoft OneNote Informatio n Disclosure Vulnerability."

CVE ID: CVE-2017-0197
Severity: CRITICAL
Description: Microsoft OneNote 2007 SP3 and Microsoft OneNote 2010 SP2 allow remote attackers to execute arbit rary code via a crafted document, aka "Microsoft Office DLL Loading Vulnerability."

Microsoft Excel 12.0.4518.1014 (update available)

CVE ID: CVE-2007-0215
Severity: IMPORTANT
Description: Stack-based buffer overflow in Microsoft Excel 2000 SP3, 2002 SP3, 2003 SP2, and 2003 Viewer allow s user-assisted remote attackers to execute arbitrary code via a .XLS BIFF file with a malformed Named Graph record, which results in memory corruption.

CVE ID: CVE-2007-1203
Severity: CRITICAL
Description: Unspecified vulnerability in Microsoft Excel 2000 SP3, 2002 SP3, 2003 SP2, 2003 Viewer, 2004 for Ma c, and 2007 allows user-assisted remote attackers to execute arbitrary code via a crafted set font value i n an Excel file, which results in memory corruption.

CVE ID: CVE-2007-1756
Severity: CRITICAL
Description: Microsoft Excel 2000 SP3, 2002 SP3, 2003 SP2, 2003 Viewer, and Office Excel 2007 does not properly validate version information, which allows user-assisted remote attackers to execute arbitrary code via a crafted Excel file, aka "Calculation Error Vulnerability".

CVE ID: CVE-2007-3030
Severity: IMPORTANT
Description: Microsoft Excel 2000 SP3, 2002 SP3, 2003 SP2, and 2003 Viewer allows user-assisted remote attacke rs to execute arbitrary code via a malformed Excel file involving the "denoting [of] the start of a Workspa ce designation", which results in memory corruption, aka the "Workbook Memory Corruption Vulnerabilit y".

CVE ID: CVE-2008-0115
Severity: CRITICAL
Description: Unspecified vulnerability in Microsoft Excel 2000 SP3 through 2007, Viewer 2003, Compatibility Pack, a nd Office for Mac 2004 allows user-assisted remote attackers to execute arbitrary code via malformed fo rmulas, aka "Excel Formula Parsing Vulnerability."

CVE ID: CVE-2008-0117

Severity: CRITICAL
Description: Unspecified vulnerability in Microsoft Excel 2000 SP3 and 2002 SP2, and Office 2004 and 2008 for Mac, allows user-assisted remote attackers to execute arbitrary code via crafted conditional formatting values, aka "Excel Conditional Formatting Vulnerability."

CVE ID: CVE-2008-3068
Severity: IMPORTANT
Description: Microsoft Crypto API 5.131.2600.2180 through 6.0, as used in Outlook, Windows Live Mail, and Office 2007, performs Certificate Revocation List (CRL) checks by using an arbitrary URL from a certificate embedded in a (1) S/MIME e-mail message or (2) signed document, which allows remote attackers to obtain reading times and IP addresses of recipients, and port-scan results, via a crafted certificate with an Authority Information Access (AIA) extension.

CVE ID: CVE-2011-0977
Severity: CRITICAL
Description: Use-after-free vulnerability in Microsoft Office XP SP3, Office 2003 SP3, Office 2007 SP2, Office 2004 and 2008 for Mac, and Open XML File Format Converter for Mac allows remote attackers to execute arbitrary code via malformed shape data in the Office drawing file format, aka "Microsoft Office Graphic Object Dereferencing Vulnerability."

CVE ID: CVE-2012-5672
Severity: MODERATE
Description: Microsoft Excel Viewer (aka Xlview.exe) and Excel in Microsoft Office 2007 (aka Office 12) allow remote attackers to cause a denial of service (read access violation and application crash) via a crafted spreadsheet file, as demonstrated by a .xls file with battery voltage data.

CVE ID: CVE-2010-3232
Severity: CRITICAL
Description: Microsoft Excel 2003 SP3 and 2007 SP2; Office 2004 and 2008 for Mac; Open XML File Format Converter for Mac; Excel Viewer SP2; and Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats SP2 do not properly validate record information, which allows remote attackers to execute arbitrary code via a crafted Excel document, aka "Excel File Format Parsing Vulnerability."

CVE ID: CVE-2012-0141
Severity: CRITICAL
Description: Microsoft Excel 2003 SP3, 2007 SP2 and SP3, and 2010 Gold and SP1; Office 2011 for Mac; Excel Viewer; and Office Compatibility Pack SP2 and SP3 do not properly handle memory during the opening of files, which allows remote attackers to execute arbitrary code via a crafted spreadsheet, aka "Excel File Format Memory Corruption Vulnerability."

CVE ID: CVE-2012-0142
Severity: CRITICAL
Description: Microsoft Excel 2003 SP3, 2007 SP2 and SP3, and 2010 Gold and SP1; Office 2008 for Mac; Excel Viewer; and Office Compatibility Pack SP2 and SP3 do not properly handle memory during the opening of files, which allows remote attackers to execute arbitrary code via a crafted spreadsheet, aka "Excel File Format Memory Corruption in OBJECTLINK Record Vulnerability."

CVE ID: CVE-2012-0184
Severity: CRITICAL
Description: Microsoft Excel 2003 SP3, 2007 SP2 and SP3, and 2010 Gold and SP1; Office 2008 and 2011 for Mac; Excel Viewer; and Office Compatibility Pack SP2 and SP3 do not properly handle memory during the opening of files, which allows remote attackers to execute arbitrary code via a crafted spreadsheet, aka "Excel SXLI Record Memory Corruption Vulnerability."

CVE ID: CVE-2012-1847
Severity: CRITICAL
Description: Microsoft Excel 2003 SP3, 2007 SP2 and SP3, and 2010 Gold and SP1; Office 2008 and 2011 for Mac; Excel Viewer; and Office Compatibility Pack SP2 and SP3 do not properly handle memory during the opening of files, which allows remote attackers to execute arbitrary code via a crafted spreadsheet, aka "Excel Series Record Parsing Type Mismatch Could Result in Remote Code Execution Vulnerability."

CVE ID: CVE-2012-1885
Severity: CRITICAL
Description: Heap-based buffer overflow in Microsoft Excel 2003 SP3, 2007 SP2 and SP3, and 2010 SP1; Office 2008 and 2011 for Mac; and Office Compatibility Pack SP2 and SP3 allows remote attackers to execute arbitrary code via a crafted spreadsheet, aka "Excel SerAuxErrBar Heap Overflow Vulnerability."

CVE ID: CVE-2012-1886

Severity: CRITICAL
Description: Microsoft Excel 2003 SP3, 2007 SP2 and SP3, and 2010 SP1; Excel Viewer; and Office Compatibility P ack SP2 and SP3 allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted spreadsheet, aka "Excel Memory Corruption Vulnerability."

CVE ID: CVE-2012-1887
Severity: CRITICAL
Description: Use-after-free vulnerability in Microsoft Excel 2003 SP3, 2007 SP2 and SP3, and 2010 SP1, and Office 2008 and 2011 for Mac, allows remote attackers to execute arbitrary code via a crafted spreadsheet, ak a "Excel SST Invalid Length Use After Free Vulnerability."

CVE ID: CVE-2013-1315
Severity: CRITICAL
Description: Microsoft SharePoint Server 2007 SP3, 2010 SP1 and SP2, and 2013; Office Web Apps 2010; Excel 2 003 SP3, 2007 SP3, 2010 SP1 and SP2, 2013, and 2013 RT; Office for Mac 2011; Excel Viewer; and O ffice Compatibility Pack SP3 allow remote attackers to execute arbitrary code or cause a denial of servic e (memory corruption) via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerab ility."

CVE ID: CVE-2013-3158
Severity: CRITICAL
Description: Microsoft Excel 2003 SP3 and 2007 SP3 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted Office document, aka "Microsoft Office Memory Corr uption Vulnerability."

CVE ID: CVE-2013-3159
Severity: MODERATE
Description: Microsoft Excel 2003 SP3, 2007 SP3, and 2010 SP1 and SP2; Excel Viewer; and Microsoft Office Com patibility Pack SP3 allow remote attackers to read arbitrary files via an XML document containing an ext ernal entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) i ssue, aka "XML External Entities Resolution Vulnerability."

CVE ID: CVE-2012-0185
Severity: CRITICAL
Description: Heap-based buffer overflow in Microsoft Excel 2007 SP2 and SP3 and 2010 Gold and SP1, Excel View er, and Office Compatibility Pack SP2 and SP3 allows remote attackers to execute arbitrary code via a c rafted spreadsheet that triggers incorrect handling of memory during opening, aka "Excel MergeCells Re cord Heap Overflow Vulnerability."

CVE ID: CVE-2012-2543
Severity: CRITICAL
Description: Stack-based buffer overflow in Microsoft Excel 2007 SP2 and SP3 and 2010 SP1; Office 2011 for Mac; Excel Viewer; and Office Compatibility Pack SP2 and SP3 allows remote attackers to execute arbitrary c ode via a crafted spreadsheet, aka "Excel Stack Overflow Vulnerability."

CVE ID: CVE-2013-3890
Severity: CRITICAL
Description: Microsoft Excel 2007 SP3, Excel Viewer, and Office Compatibility Pack SP3 allow remote attackers to e xecute arbitrary code via a crafted Office document, aka "Microsoft Excel Memory Corruption Vulnerabili ty."

CVE ID: CVE-2014-6360
Severity: CRITICAL
Description: Microsoft Excel 2007 SP3, Excel 2010 SP2, and Office Compatibility Pack allow remote attackers to ex ecute arbitrary code via a crafted Office document, aka "Global Free Remote Code Execution in Excel V ulnerability."

CVE ID: CVE-2014-6361
Severity: CRITICAL
Description: Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 Gold and SP1, Excel 2013 RT Gold and SP1, and Office Compatibility Pack allow remote attackers to execute arbitrary code via a crafted Office docu ment, aka "Excel Invalid Pointer Remote Code Execution Vulnerability."

CVE ID: CVE-2015-0063
Severity: CRITICAL
Description: Microsoft Excel 2007 SP3; the proofing tools in Office 2010 SP2; Excel 2010 SP2; Excel 2013 Gold, SP 1, and RT; Excel Viewer; and Office Compatibility Pack SP3 allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted Office document, aka "Excel Remot

e Code Execution Vulnerability."

CVE ID: CVE-2015-0085
Severity: CRITICAL
Description: Use-after-free vulnerability in Microsoft Office 2007 SP3, Excel 2007 SP3, PowerPoint 2007 SP3, Word 2007 SP3, Office 2010 SP2, Excel 2010 SP2, PowerPoint 2010 SP2, Word 2010 SP2, Office 2013 Gold and SP1, Word 2013 Gold and SP1, Office 2013 RT Gold and SP1, Word 2013 RT Gold and SP1, Excel Viewer, Office Compatibility Pack SP3, Word Automation Services on SharePoint Server 2010 SP2, Excel Services on SharePoint Server 2013 Gold and SP1, Word Automation Services on SharePoint Server 2013 Gold and SP1, Web Applications 2010 SP2, Office Web Apps Server 2010 SP2, Web Apps Server 2013 Gold and SP1, SharePoint Server 2007 SP3, Windows SharePoint Services 3.0 SP3, SharePoint Foundation 2010 SP2, SharePoint Server 2010 SP2, SharePoint Foundation 2013 Gold and SP1, and SharePoint Server 2013 Gold and SP1 allows remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Component Use After Free Vulnerability."

CVE ID: CVE-2015-0097
Severity: CRITICAL
Description: Microsoft Excel 2007 SP3, PowerPoint 2007 SP3, Word 2007 SP3, Excel 2010 SP2, PowerPoint 2010 SP2, and Word 2010 SP2 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Word Local Zone Remote Code Execution Vulnerability."

CVE ID: CVE-2015-2376
Severity: CRITICAL
Description: Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Office for Mac 2011, Excel Viewer 2007 SP3, Office Compatibility Pack SP3, Excel Services on SharePoint Server 2007 SP3, Excel Services on SharePoint Server 2010 SP2, and Excel Services on SharePoint Server 2013 SP1 allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."

CVE ID: CVE-2015-2377
Severity: CRITICAL
Description: Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, and Office Compatibility Pack SP3 allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."

CVE ID: CVE-2015-2378
Severity: IMPORTANT
Description: Untrusted search path vulnerability in Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel Viewer 2007 SP3, and Office Compatibility Pack SP3 allows local users to gain privileges via a Trojan horse DLL in the current working directory, aka "Microsoft Excel DLL Remote Code Execution Vulnerability."

CVE ID: CVE-2015-2415
Severity: CRITICAL
Description: Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, and Office Compatibility Pack SP3 allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."

CVE ID: CVE-2015-2423
Severity: MODERATE
Description: Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, Windows 10, Excel 2007 SP3, PowerPoint 2007 SP3, Visio 2007 SP3, Word 2007 SP3, Office 2010 SP2, Excel 2010 SP2, PowerPoint 2010 SP2, Visio 2010 SP2, Word 2010 SP2, Excel 2013 SP1, PowerPoint 2013 SP1, Visio 2013 SP1, Word 2013 SP1, Excel 2013 RT SP1, PowerPoint 2013 RT SP1, Visio 2013 RT SP1, Word 2013 RT SP1, and Internet Explorer 7 through 11 allow remote attackers to gain privileges and obtain sensitive information via a crafted command-line parameter to an Office application or Notepad, as demonstrated by a transition from Low Integrity to Medium Integrity, aka "Unsafe Command Line Parameter Passing Vulnerability."

CVE ID: CVE-2015-2435
Severity: CRITICAL
Description: Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, Windows 10, Office 2007 SP3 and 2010 SP2, Live Meeting 2007 Console, Lync 2010, Lync 2010 Attendee, Lync 2013 SP1, Lync Basic 2013 SP1, and Silverlight before 5.1.40728 allow remote attackers to execute arbitrary code via a crafted TrueType font, aka "TrueType Font Parsing Vulnerability."

CVE ID: CVE-2015-2503

Severity: CRITICAL
Description: Microsoft Access 2007 SP3, Excel 2007 SP3, InfoPath 2007 SP3, OneNote 2007 SP3, PowerPoint 2007 SP3, Project 2007 SP3, Publisher 2007 SP3, Visio 2007 SP3, Word 2007 SP3, Office 2007 IME (Japanese) SP3, Access 2010 SP2, Excel 2010 SP2, InfoPath 2010 SP2, OneNote 2010 SP2, PowerPoint 2010 SP2, Project 2010 SP2, Publisher 2010 SP2, Visio 2010 SP2, Word 2010 SP2, Pinyin IME 2010, Access 2013 SP1, Excel 2013 SP1, InfoPath 2013 SP1, OneNote 2013 SP1, PowerPoint 2013 SP1, Project 2013 SP1, Publisher 2013 SP1, Visio 2013 SP1, Word 2013 SP1, Excel 2013 RT SP1, OneNote 2013 RT SP1, PowerPoint 2013 RT SP1, Word 2013 RT SP1, Access 2016, Excel 2016, OneNote 2016, PowerPoint 2016, Project 2016, Publisher 2016, Visio 2016, Word 2016, Skype for Business 2016, and Lync 2013 SP1 allow remote attackers to bypass a sandbox protection mechanism and gain privileges via a crafted web site that is accessed with Internet Explorer, as demonstrated by a transition from Low Integrity to Medium Integrity, aka "Microsoft Office Elevation of Privilege Vulnerability."

CVE ID: CVE-2015-2520
Severity: CRITICAL
Description: Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel for Mac 2011 and 2016, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."

CVE ID: CVE-2015-2521
Severity: CRITICAL
Description: Microsoft Excel 2007 SP3, Excel 2010 SP2, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."

CVE ID: CVE-2015-2523
Severity: CRITICAL
Description: Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel for Mac 2011 and 2016, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."

CVE ID: CVE-2015-2558
Severity: CRITICAL
Description: Use-after-free vulnerability in Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2016, Excel for Mac 2011, Excel 2016 for Mac, Excel Viewer, Office Compatibility Pack SP3, and Excel Services on SharePoint Server 2007 SP3, 2010 SP2, and 2013 SP1 allows remote attackers to execute arbitrary code via a long fileVersion element in an Office document, aka "Microsoft Office Memory Corruption Vulnerability."

CVE ID: CVE-2015-6038
Severity: CRITICAL
Description: Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2016, Excel for Mac 2011, Excel 2016 for Mac, Office Compatibility Pack SP3, Excel Viewer, and Excel Services on SharePoint Server 2007 SP3, 2010 SP2, and 2013 SP1 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."

CVE ID: CVE-2015-6040
Severity: CRITICAL
Description: Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel for Mac 2011, Excel 2016 for Mac, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."

CVE ID: CVE-2015-6122
Severity: CRITICAL
Description: Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel for Mac 2011, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."

CVE ID: CVE-2015-6177
Severity: CRITICAL
Description: Microsoft Excel 2007 SP3, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."

CVE ID: CVE-2016-0012
Severity: MODERATE
Description: Microsoft Office 2007 SP3, Excel 2007 SP3, PowerPoint 2007 SP3, Visio 2007 SP3, Word 2007 SP3, Office 2010 SP2, Excel 2010 SP2, PowerPoint 2010 SP2, Visio 2010 SP2, Word 2010 SP2, Office 2013

SP1, Excel 2013 SP1, PowerPoint 2013 SP1, Visio 2013 SP1, Word 2013 SP1, Excel 2013 RT SP1, PowerPoint 2013 RT SP1, Word 2013 RT SP1, Office 2016, Excel 2016, PowerPoint 2016, Visio 2016, Word 2016, and Visual Basic 6.0 Runtime allow remote attackers to bypass the ASLR protection mechanism via unspecified vectors, aka "Microsoft Office ASLR Bypass."

CVE ID: CVE-2016-0035
Severity: CRITICAL
Description: Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2016, Excel for Mac 2011, Excel 2016 for Mac, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."

CVE ID: CVE-2016-0054
Severity: CRITICAL
Description: Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2016, Excel for Mac 2011, Excel 2016 for Mac, Office Compatibility Pack SP3, Excel Viewer, Excel Services on SharePoint Server 2007 SP3, Excel Services on SharePoint Server 2010 SP2, Excel Services on SharePoint Server 2013 SP1, and Office Web Apps 2010 SP2 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."

CVE ID: CVE-2016-0122
Severity: CRITICAL
Description: Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2016, Word 2016 for Mac, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."

CVE ID: CVE-2016-0136
Severity: CRITICAL
Description: Microsoft Excel 2007 SP3, Excel 2010 SP2, Office Compatibility Pack SP3, Excel Services on SharePoint Server 2007 SP3, and Excel Services on SharePoint Server 2010 SP2 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."

CVE ID: CVE-2016-3233
Severity: CRITICAL
Description: Microsoft Excel 2007 SP3, Excel 2010 SP2, and Office Compatibility Pack SP3 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."

CVE ID: CVE-2016-3284
Severity: CRITICAL
Description: Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2016, Excel for Mac 2011, Excel 2016 for Mac, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."

CVE ID: CVE-2016-3358
Severity: CRITICAL
Description: Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2016, Excel 2016 for Mac, Office Compatibility Pack SP3, Excel Viewer, Excel Services on SharePoint Server 2007 SP3, Excel Services on SharePoint Server 2010 SP2, Excel Automation Services on SharePoint Server 2013 SP1, and Office Online Server allow remote attackers to execute arbitrary code via a crafted document, aka "Microsoft Office Memory Corruption Vulnerability."

CVE ID: CVE-2016-3359
Severity: CRITICAL
Description: Microsoft Excel 2007 SP3, Excel 2010 SP2, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code via a crafted document, aka "Microsoft Office Memory Corruption Vulnerability."

CVE ID: CVE-2016-3362
Severity: CRITICAL
Description: Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2016, Office Compatibility Pack SP3, Excel Viewer, Excel Services on SharePoint Server 2007 SP3, Excel Services on SharePoint Server 2010 SP2, Excel Automation Services on SharePoint Server 2013 SP1, and Office Online Server allow remote attackers to execute arbitrary code via a crafted document, aka "Microsoft Office Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3365.

CVE ID: CVE-2016-3363

Severity: CRITICAL
Description: Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2016, Office C ompatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code via a crafted d ocument, aka "Microsoft Office Memory Corruption Vulnerability," a different vulnerability than CVE-201 6-3381.

CVE ID: CVE-2016-3365
Severity: CRITICAL
Description: Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2016, Office C ompatibility Pack SP3, Excel Viewer, Excel Services on SharePoint Server 2007 SP3, Excel Services o n SharePoint Server 2010 SP2, Excel Automation Services on SharePoint Server 2013 SP1, and Office Online Server allow remote attackers to execute arbitrary code via a crafted document, aka "Microsoft O ffice Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3362.

CVE ID: CVE-2016-3381
Severity: CRITICAL
Description: Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2016, Office C ompatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code via a crafted d ocument, aka "Microsoft Office Memory Corruption Vulnerability," a different vulnerability than CVE-201 6-3363.

CVE ID: CVE-2016-7213
Severity: CRITICAL
Description: Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2016, Excel fo r Mac 2011, Excel 2016 for Mac, and Office Compatibility Pack SP3 allow remote attackers to execute a rbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."

CVE ID: CVE-2016-7228
Severity: CRITICAL
Description: Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2016, Excel fo r Mac 2011, Excel 2016 for Mac, and Office Compatibility Pack SP3 allow remote attackers to execute a rbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."

CVE ID: CVE-2016-7229
Severity: CRITICAL
Description: Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2016, Excel fo r Mac 2011, Excel 2016 for Mac, Office Compatibility Pack SP3, and Excel Viewer allow remote attacker s to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vuln erability."

CVE ID: CVE-2016-7231
Severity: CRITICAL
Description: Microsoft Excel 2007 SP3, Excel for Mac 2011, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."

CVE ID: CVE-2016-7262
Severity: IMPORTANT
Description: Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2016, Office C ompatibility Pack SP3, and Excel Viewer allow user-assisted remote attackers to execute arbitrary com mands via a crafted cell that is mishandled upon a click, aka "Microsoft Office Security Feature Bypass Vulnerability."

CVE ID: CVE-2016-7264
Severity: MODERATE
Description: Microsoft Excel 2007 SP3, Office Compatibility Pack SP3, Excel Viewer, Excel for Mac 2011, and Excel 2016 for Mac allow remote attackers to obtain sensitive information from process memory or cause a de nial of service (out-of-bounds read) via a crafted document, aka "Microsoft Office Information Disclosure Vulnerability."

CVE ID: CVE-2016-7265
Severity: MODERATE
Description: Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2016, Office C ompatibility Pack SP3, Excel Viewer, Excel Services on SharePoint Server 2007 SP3, and Excel Servic es on SharePoint Server 2010 SP2 allow remote attackers to obtain sensitive information from process memory or cause a denial of service (out-of-bounds read) via a crafted document, aka "Microsoft Office Information Disclosure Vulnerability."

CVE ID: CVE-2016-7266
Severity: IMPORTANT
Description: Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2016, Office C ompatibility Pack SP3, Excel Viewer, and Excel 2016 for Mac mishandle a registry check, which allows user-assisted remote attackers to execute arbitrary commands via crafted embedded content in a docu ment, aka "Microsoft Office Security Feature Bypass Vulnerability."

CVE ID: CVE-2017-0006
Severity: CRITICAL
Description: Microsoft Excel 2007 SP3, Office Compatibility Pack SP3, Excel Viewer, and Excel Services on ShareP oint Server 2007 SP3 allow remote attackers to execute arbitrary code or cause a denial of service (me mory corruption) via a crafted document, aka "Microsoft Office Memory Corruption Vulnerability." This v ulnerability is different from those described in CVE-2017-0019, CVE-2017-0020, CVE-2017-0030, CVE -2017-0031, CVE-2017-0052, and CVE-2017-0053.

CVE ID: CVE-2017-0027
Severity: LOW
Description: Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 RT SP1, Excel 2016, Office Compatibility Pack SP3, and Excel Services on SharePoint Server 2013 SP1 allow remote attackers to obtain sensitive info rmation from process memory via a crafted Office document, aka "Microsoft Office Information Disclosur e Vulnerability."

CVE ID: CVE-2017-0052
Severity: CRITICAL
Description: Microsoft Office Compatibility Pack SP3, Excel 2007 SP3, Excel Viewer, and Excel Services on ShareP oint Server 2007 SP3 allow remote attackers to execute arbitrary code or cause a denial of service (me mory corruption) via a crafted document, aka "Microsoft Office Memory Corruption Vulnerability." This v ulnerability is different from those described in CVE-2017-0006, CVE-2017-0019, CVE-2017-0020, CVE -2017-0030, CVE-2017-0031, and CVE-2017-0053.

CVE ID: CVE-2017-0194
Severity: MODERATE
Description: Microsoft Excel 2007 SP3, Microsoft Excel 2010 SP2, and Office Compatibility Pack SP2 allow remote attackers to obtain sensitive information from process memory via a crafted Office document, aka "Micro soft Office Information Disclosure Vulnerability."

Microsoft Word 12.0.4518.1014 (update available)
CVE ID: CVE-2008-1092
Severity: CRITICAL
Description: Buffer overflow in msjet40.dll before 4.0.9505.0 in Microsoft Jet Database Engine allows remote attacke rs to execute arbitrary code via a crafted Word file, as exploited in the wild in March 2008. NOTE: as of 20080513, Microsoft has stated that this is the same issue as CVE-2007-6026.

CVE ID: CVE-2007-1910
Severity: IMPORTANT
Description: Buffer overflow in wwlib.dll in Microsoft Word 2007 allows remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via a crafted document, as demonstrated by file7 89-1.doc.

CVE ID: CVE-2007-1911
Severity: IMPORTANT
Description: Multiple unspecified vulnerabilities in Microsoft Word 2007 allow remote attackers to cause a denial of s ervice (CPU consumption) via crafted documents, as demonstrated by (1) file798-1.doc and (2) file613- 1.doc, possibly related to a buffer overflow.

CVE ID: CVE-2008-6063
Severity: MODERATE
Description: Microsoft Word 2007, when the "Save as PDF" add-on is enabled, places an absolute pathname in the Subject field during an "Email as PDF" operation, which allows remote attackers to obtain sensitive infor mation such as the sender’s account name and a Temporary Internet Files subdirectory name.

CVE ID: CVE-2016-7232
Severity: CRITICAL
Description: Microsoft Word 2007, Office 2010 SP2, Word 2010 SP2, Word for Mac 2011, and Office Compatibility P ack SP3 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."

CVE ID: CVE-2016-7233

Severity: MODERATE
Description: Microsoft Word 2007, Office 2010 SP2, Word 2010 SP2, Word for Mac 2011, Excel for Mac 2011, Word Viewer, Office Compatibility Pack SP3, Word Automation Services on SharePoint Server 2013 SP1, and Office Web Apps 2010 SP2 allow remote attackers to obtain sensitive information from process memory or cause a denial of service (out-of-bounds read) via a crafted Office document, aka "Microsoft Office Information Disclosure Vulnerability."

CVE ID: CVE-2016-7234
Severity: CRITICAL
Description: Microsoft Word 2007, Office 2010 SP2, Word 2010 SP2, Word 2013 SP1, Word 2013 RT SP1, Word for Mac 2011, Excel for Mac 2011, Word 2016 for Mac, Office Compatibility Pack SP3, Word Automation Services on SharePoint Server 2010 SP2, Word Automation Services on SharePoint Server 2013 SP1, Office Web Apps 2010 SP2, and Office Web Apps Server 2013 SP1 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."

CVE ID: CVE-2016-7235
Severity: CRITICAL
Description: Microsoft Word 2007, Office 2010 SP2, Word 2010 SP2, Word for Mac 2011, Excel for Mac 2011, and Office Compatibility Pack SP3 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."

CVE ID: CVE-2012-0183
Severity: CRITICAL
Description: Microsoft Word 2003 SP3 and 2007 SP2 and SP3, Office 2008 and 2011 for Mac, and Office Compatibility Pack SP2 and SP3 allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted RTF data, aka "RTF Mismatch Vulnerability."

CVE ID: CVE-2012-2528
Severity: CRITICAL
Description: Use-after-free vulnerability in Microsoft Word 2003 SP3, 2007 SP2 and SP3, and 2010 SP1; Word Viewer; Office Compatibility Pack SP2 and SP3; Word Automation Services on Microsoft SharePoint Server 2010; and Office Web Apps 2010 SP1 allows remote attackers to execute arbitrary code via a crafted RTF document, aka "RTF File listid Use-After-Free Vulnerability."

CVE ID: CVE-2012-2539
Severity: CRITICAL
Description: Microsoft Word 2003 SP3, 2007 SP2 and SP3, and 2010 SP1; Word Viewer; Office Compatibility Pack SP2 and SP3; and Office Web Apps 2010 SP1 allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted RTF data, aka "Word RTF 'listoverridecount' Remote Code Execution Vulnerability."

CVE ID: CVE-2013-3160
Severity: MODERATE
Description: Microsoft Office 2003 SP3 and 2007 SP3, Word 2003 SP3 and 2007 SP3, and Word Viewer allow remote attackers to read arbitrary files via an XML document containing an external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue, aka "XML External Entities Resolution Vulnerability."

CVE ID: CVE-2013-3847
Severity: CRITICAL
Description: Microsoft Word Automation Services in SharePoint Server 2010 SP1, Word Web App 2010 SP1 in Office Web Apps 2010, Word 2003 SP3, Word 2007 SP3, Word 2010 SP1, Office Compatibility Pack SP3, and Word Viewer allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted Office document, aka "Word Memory Corruption Vulnerability," a different vulnerability than CVE-2013-3848, CVE-2013-3849, and CVE-2013-3858.

CVE ID: CVE-2013-3848
Severity: CRITICAL
Description: Microsoft Word Automation Services in SharePoint Server 2010 SP1, Word Web App 2010 SP1 in Office Web Apps 2010, Word 2003 SP3, Word 2007 SP3, Word 2010 SP1, Office Compatibility Pack SP3, and Word Viewer allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted Office document, aka "Word Memory Corruption Vulnerability," a different vulnerability than CVE-2013-3847, CVE-2013-3849, and CVE-2013-3858.

CVE ID: CVE-2013-3849
Severity: CRITICAL
Description: Microsoft Word Automation Services in SharePoint Server 2010 SP1, Word Web App 2010 SP1 in Office Web Apps 2010, Word 2003 SP3, Word 2007 SP3, Word 2010 SP1, Office Compatibility Pack SP3, a

nd Word Viewer allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted Office document, aka "Word Memory Corruption Vulnerability," a different vulne rability than CVE-2013-3847, CVE-2013-3848, and CVE-2013-3858.

CVE ID: CVE-2013-3850
Severity: CRITICAL
Description: Microsoft Word 2003 SP3, 2007 SP3, and 2010 SP1 and SP2; Office Compatibility Pack SP3; and Wor d Viewer allow remote attackers to execute arbitrary code or cause a denial of service (memory corrupti on) via a crafted Office document, aka "Word Memory Corruption Vulnerability."

CVE ID: CVE-2013-3851
Severity: CRITICAL
Description: Microsoft Office 2003 SP3 and 2007 SP3, Word 2003 SP3 and 2007 SP3, Office Compatibility Pack SP 3, and Word Viewer allow remote attackers to execute arbitrary code or cause a denial of service (mem ory corruption) via a crafted Office document, aka "Word Memory Corruption Vulnerability."

CVE ID: CVE-2013-3852
Severity: CRITICAL
Description: Microsoft Word 2003 SP3, 2007 SP3, and 2010 SP1; Office Compatibility Pack SP3; and Word Viewer allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted Office document, aka "Word Memory Corruption Vulnerability."

CVE ID: CVE-2013-3855
Severity: CRITICAL
Description: Microsoft Word 2003 SP3 and 2007 SP3, Office Compatibility Pack SP3, and Word Viewer allow remot e attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted Offic e document, aka "Word Memory Corruption Vulnerability."

CVE ID: CVE-2013-3857
Severity: CRITICAL
Description: Microsoft Word Automation Services in SharePoint Server 2010 SP1 and SP2, Word Web App 2010 S P1 and SP2 in Office Web Apps 2010, Word 2003 SP3, Word 2007 SP3, Word 2010 SP1 and SP2, Offi ce Compatibility Pack SP3, and Word Viewer allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted Office document, aka "Word Memory Corruption V ulnerability."

CVE ID: CVE-2013-3858
Severity: CRITICAL
Description: Microsoft Word Automation Services in SharePoint Server 2010 SP1, Word Web App 2010 SP1 in Offic e Web Apps 2010, Word 2003 SP3, Word 2007 SP3, Word 2010 SP1, Office Compatibility Pack SP3, a nd Word Viewer allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted Office document, aka "Word Memory Corruption Vulnerability," a different vulne rability than CVE-2013-3847, CVE-2013-3848, and CVE-2013-3849.

CVE ID: CVE-2014-0258
Severity: CRITICAL
Description: Microsoft Word 2003 SP3 and 2007 SP3, Office Compatibility Pack SP3, and Word Viewer allow remot e attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted Offic e document, aka "Word Memory Corruption Vulnerability."

CVE ID: CVE-2014-0260
Severity: CRITICAL
Description: Microsoft Word 2003 SP3, 2007 SP3, 2010 SP1 and SP2, 2013, and 2013 RT; Office Compatibility Pac k SP3; Word Viewer; SharePoint Server 2010 SP1 and SP2 and 2013; Office Web Apps 2010 SP1 and SP2; and Office Web Apps Server 2013 allow remote attackers to execute arbitrary code or cause a den ial of service (memory corruption) via a crafted Office document, aka "Word Memory Corruption Vulnera bility."

CVE ID: CVE-2014-1761
Severity: CRITICAL
Description: Microsoft Word 2003 SP3, 2007 SP3, 2010 SP1 and SP2, 2013, and 2013 RT; Word Viewer; Office Co mpatibility Pack SP3; Office for Mac 2011; Word Automation Services on SharePoint Server 2010 SP1 and SP2 and 2013; Office Web Apps 2010 SP1 and SP2; and Office Web Apps Server 2013 allow remo te attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted RTF data, as exploited in the wild in March 2014.

CVE ID: CVE-2012-0182
Severity: CRITICAL

Description: Microsoft Word 2007 SP2 and SP3 does not properly handle memory during the parsing of Word docu ments, which allows remote attackers to execute arbitrary code via a crafted document, aka "Word PAP X Section Corruption Vulnerability."

CVE ID: CVE-2013-3853
Severity: CRITICAL
Description: Microsoft Office 2007 SP3 and Word 2007 SP3 allow remote attackers to execute arbitrary code or cau se a denial of service (memory corruption) via a crafted Office document, aka "Word Memory Corruption Vulnerability," a different vulnerability than CVE-2013-3854.

CVE ID: CVE-2013-3854
Severity: CRITICAL
Description: Microsoft Office 2007 SP3 and Word 2007 SP3 allow remote attackers to execute arbitrary code or cau se a denial of service (memory corruption) via a crafted Office document, aka "Word Memory Corruption Vulnerability," a different vulnerability than CVE-2013-3853.

CVE ID: CVE-2013-3892
Severity: CRITICAL
Description: Microsoft Word 2007 SP3 and Office Compatibility Pack SP3 allow remote attackers to execute arbitrar y code via a crafted Office document, aka "Memory Corruption Vulnerability."

CVE ID: CVE-2014-0259
Severity: CRITICAL
Description: Microsoft Word 2007 SP3 and Office Compatibility Pack SP3 allow remote attackers to execute arbitrar y code or cause a denial of service (memory corruption) via a crafted Office document, aka "Word Mem ory Corruption Vulnerability."

CVE ID: CVE-2014-1757
Severity: CRITICAL
Description: Microsoft Word 2007 SP3 and 2010 SP1 and SP2, and Office Compatibility Pack SP3, allocates memor y incorrectly for file conversions from a binary (aka .doc) format to a newer format, which allows remote attackers to execute arbitrary code via a crafted document, aka "Microsoft Office File Format Converter Vulnerability."

CVE ID: CVE-2014-2778
Severity: CRITICAL
Description: Microsoft Word 2007 SP3 and Office Compatibility Pack SP3 allow remote attackers to execute arbitrar y code or cause a denial of service (memory corruption) via a crafted embedded font in a (1) .doc or (2) .docx document, aka "Embedded Font Vulnerability."

CVE ID: CVE-2014-6333
Severity: CRITICAL
Description: Microsoft Word 2007 SP3, Word Viewer, and Office Compatibility Pack SP3 allow remote attackers to e xecute arbitrary code via a crafted Office document, aka "Microsoft Office Double Delete Remote Code Execution Vulnerability."

CVE ID: CVE-2014-6334
Severity: CRITICAL
Description: Microsoft Word 2007 SP3, Word Viewer, and Office Compatibility Pack SP3 allow remote attackers to e xecute arbitrary code or cause a denial of service (memory corruption) via a crafted Office document, ak a "Microsoft Office Bad Index Remote Code Execution Vulnerability."

CVE ID: CVE-2014-6335
Severity: CRITICAL
Description: Microsoft Word 2007 SP3, Word Viewer, and Office Compatibility Pack SP3 allow remote attackers to e xecute arbitrary code or cause a denial of service (memory corruption) via a crafted Office document, ak a "Microsoft Office Invalid Pointer Remote Code Execution Vulnerability."

CVE ID: CVE-2014-6356
Severity: CRITICAL
Description: Array index error in Microsoft Word 2007 SP3, Word 2010 SP2, and Office Compatibility Pack SP3 allo ws remote attackers to execute arbitrary code via a crafted Office document, aka "Invalid Index Remote Code Execution Vulnerability."

CVE ID: CVE-2015-0064
Severity: CRITICAL
Description: Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Word Automation Services in SharePoint Server 2010, Web Applications 2010 SP2, Word Viewer, and Office Compatibility Pack SP3 allow remot

e attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted Offic e document, aka "Office Remote Code Execution Vulnerability."

CVE ID: CVE-2015-0065
Severity: CRITICAL
Description: Microsoft Word 2007 SP3 allows remote attackers to execute arbitrary code or cause a denial of servic e (memory corruption) via a crafted Office document, aka "OneTableDocumentStream Remote Code Ex ecution Vulnerability."

CVE ID: CVE-2015-0085
Severity: CRITICAL
Description: Use-after-free vulnerability in Microsoft Office 2007 SP3, Excel 2007 SP3, PowerPoint 2007 SP3, Word 2007 SP3, Office 2010 SP2, Excel 2010 SP2, PowerPoint 2010 SP2, Word 2010 SP2, Office 2013 Gold and SP1, Word 2013 Gold and SP1, Office 2013 RT Gold and SP1, Word 2013 RT Gold and SP1, Exce l Viewer, Office Compatibility Pack SP3, Word Automation Services on SharePoint Server 2010 SP2, Ex cel Services on SharePoint Server 2013 Gold and SP1, Word Automation Services on SharePoint Serv er 2013 Gold and SP1, Web Applications 2010 SP2, Office Web Apps Server 2010 SP2, Web Apps Ser ver 2013 Gold and SP1, SharePoint Server 2007 SP3, Windows SharePoint Services 3.0 SP3, SharePo int Foundation 2010 SP2, SharePoint Server 2010 SP2, SharePoint Foundation 2013 Gold and SP1, an d SharePoint Server 2013 Gold and SP1 allows remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Component Use After Free Vulnerability."

CVE ID: CVE-2015-0086
Severity: CRITICAL
Description: Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Word 2013 Gold and SP1, Word 2013 R T Gold and SP1, Word Viewer, Office Compatibility Pack SP3, Word Automation Services on SharePoin t Server 2010 SP2, Word Automation Services on SharePoint Server 2013 Gold and SP1, Web Applicati ons 2010 SP2, and Web Apps Server 2013 Gold and SP1 allow remote attackers to execute arbitrary co de or cause a denial of service (memory corruption) via a crafted RTF document, aka "Microsoft Office Memory Corruption Vulnerability."

CVE ID: CVE-2015-0097
Severity: CRITICAL
Description: Microsoft Excel 2007 SP3, PowerPoint 2007 SP3, Word 2007 SP3, Excel 2010 SP2, PowerPoint 2010 SP2, and Word 2010 SP2 allow remote attackers to execute arbitrary code via a crafted Office documen t, aka "Microsoft Word Local Zone Remote Code Execution Vulnerability."

CVE ID: CVE-2015-1641
Severity: CRITICAL
Description: Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Word 2013 SP1, Word 2013 RT SP1, Wo rd for Mac 2011, Office Compatibility Pack SP3, Word Automation Services on SharePoint Server 2010 SP2 and 2013 SP1, and Office Web Apps Server 2010 SP2 and 2013 SP1 allow remote attackers to ex ecute arbitrary code via a crafted RTF document, aka "Microsoft Office Memory Corruption Vulnerability. "

CVE ID: CVE-2015-1649
Severity: CRITICAL
Description: Use-after-free vulnerability in Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Word View er, Office Compatibility Pack SP3, Word Automation Services on SharePoint Server 2010 SP2, and Offi ce Web Apps Server 2010 SP2 allows remote attackers to execute arbitrary code via a crafted Office do cument, aka "Microsoft Office Component Use After Free Vulnerability."

CVE ID: CVE-2015-1650
Severity: CRITICAL
Description: Use-after-free vulnerability in Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Word 2013 SP1, Word 2013 RT SP1, Word Viewer, Office Compatibility Pack SP3, Word Automation Services on S harePoint Server 2010 SP2 and 2013 SP1, and Office Web Apps Server 2010 SP2 and 2013 SP1 allow s remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Compo nent Use After Free Vulnerability."

CVE ID: CVE-2015-1651
Severity: CRITICAL
Description: Use-after-free vulnerability in Microsoft Word 2007 SP3, Word Viewer, and Office Compatibility Pack S P3 allows remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Offic e Component Use After Free Vulnerability."

CVE ID: CVE-2015-2379
Severity: CRITICAL
Description: Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Word 2013 SP1, Word 2013 RT SP1, Offi

ce for Mac 2011, and Word Viewer allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."

CVE ID: CVE-2015-2380
Severity: CRITICAL
Description: Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Word 2013 SP1, and Word 2013 RT SP1 allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."

CVE ID: CVE-2015-2423
Severity: MODERATE
Description: Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, Windows 10, Excel 2007 SP3, PowerPoint 2007 SP3, Visio 2007 SP3, Word 2007 SP3, Office 2010 SP2, Excel 2010 SP2, PowerPoint 2010 SP2, Visio 2010 SP2, Word 2010 SP2, Excel 2013 SP1, PowerPoint 2013 SP1, Visio 2013 SP1, Word 2013 SP1, Excel 2013 RT SP1, PowerPoint 2013 RT SP1, Visio 2013 RT SP1, Word 2013 RT SP1, and Internet Explorer 7 through 11 allow remote attackers to gain privileges and obtain sensitive information via a crafted command-line parameter to an Office application or Notepad, as demonstrated by a transition from Low Integrity to Medium Integrity, aka "Unsafe Command Line Parameter Passing Vulnerability."

CVE ID: CVE-2015-2424
Severity: CRITICAL
Description: Microsoft PowerPoint 2007 SP3, Word 2007 SP3, PowerPoint 2010 SP2, Word 2010 SP2, PowerPoint 2013 SP1, Word 2013 SP1, and PowerPoint 2013 RT SP1 allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."

CVE ID: CVE-2015-2468
Severity: CRITICAL
Description: Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Word 2013 SP1, Word 2013 RT SP1, Office for Mac 2011, Office for Mac 2016, Office Compatibility Pack SP3, Word Viewer, Word Automation Services on SharePoint Server 2010 SP2 and 2013 SP1, Word Web Apps 2010 SP2, and Office Web Apps Server 2013 SP1 allow remote attackers to execute arbitrary code via a crafted document, aka "Microsoft Office Memory Corruption Vulnerability."

CVE ID: CVE-2015-2469
Severity: CRITICAL
Description: Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, and Office for Mac 2011 allow remote attackers to execute arbitrary code via a crafted document, aka "Microsoft Office Memory Corruption Vulnerability."

CVE ID: CVE-2015-2470
Severity: CRITICAL
Description: Integer underflow in Microsoft Office 2007 SP3, Office 2010 SP2, Office 2013 SP1, Office 2013 RT SP1, Office for Mac 2011, and Word Viewer allows remote attackers to execute arbitrary code via a crafted document, aka "Microsoft Office Integer Underflow Vulnerability."

CVE ID: CVE-2015-2503
Severity: CRITICAL
Description: Microsoft Access 2007 SP3, Excel 2007 SP3, InfoPath 2007 SP3, OneNote 2007 SP3, PowerPoint 2007 SP3, Project 2007 SP3, Publisher 2007 SP3, Visio 2007 SP3, Word 2007 SP3, Office 2007 IME (Japanese) SP3, Access 2010 SP2, Excel 2010 SP2, InfoPath 2010 SP2, OneNote 2010 SP2, PowerPoint 2010 SP2, Project 2010 SP2, Publisher 2010 SP2, Visio 2010 SP2, Word 2010 SP2, Pinyin IME 2010, Access 2013 SP1, Excel 2013 SP1, InfoPath 2013 SP1, OneNote 2013 SP1, PowerPoint 2013 SP1, Project 2013 SP1, Publisher 2013 SP1, Visio 2013 SP1, Word 2013 SP1, Excel 2013 RT SP1, OneNote 2013 RT SP1, PowerPoint 2013 RT SP1, Word 2013 RT SP1, Access 2016, Excel 2016, OneNote 2016, PowerPoint 2016, Project 2016, Publisher 2016, Visio 2016, Word 2016, Skype for Business 2016, and Lync 2013 SP1 allow remote attackers to bypass a sandbox protection mechanism and gain privileges via a crafted web site that is accessed with Internet Explorer, as demonstrated by a transition from Low Integrity to Medium Integrity, aka "Microsoft Office Elevation of Privilege Vulnerability."

CVE ID: CVE-2015-6091
Severity: CRITICAL
Description: Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Word 2013 SP1, Word 2013 RT SP1, Word 2016, and Word Viewer allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."

CVE ID: CVE-2015-6092
Severity: CRITICAL
Description: Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Word 2013 SP1, Word 2013 RT SP1, Word 2016, Office Compatibility Pack SP3, and Word Viewer allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."

CVE ID: CVE-2015-6124
Severity: CRITICAL
Description: Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Word 2013 SP1, Word 2013 RT SP1, and Office Compatibility Pack SP3 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."

CVE ID: CVE-2015-6172
Severity: CRITICAL
Description: Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Word 2013 SP1, Word 2016, Word 2013 RT SP1, and Office Compatibility Pack SP3 allow remote attackers to execute arbitrary code via a crafted email message processed by Outlook, aka "Microsoft Office RCE Vulnerability."

CVE ID: CVE-2016-0012
Severity: MODERATE
Description: Microsoft Office 2007 SP3, Excel 2007 SP3, PowerPoint 2007 SP3, Visio 2007 SP3, Word 2007 SP3, Office 2010 SP2, Excel 2010 SP2, PowerPoint 2010 SP2, Visio 2010 SP2, Word 2010 SP2, Office 2013 SP1, Excel 2013 SP1, PowerPoint 2013 SP1, Visio 2013 SP1, Word 2013 SP1, Excel 2013 RT SP1, PowerPoint 2013 RT SP1, Word 2013 RT SP1, Office 2016, Excel 2016, PowerPoint 2016, Visio 2016, Word 2016, and Visual Basic 6.0 Runtime allow remote attackers to bypass the ASLR protection mechanism via unspecified vectors, aka "Microsoft Office ASLR Bypass."

CVE ID: CVE-2016-0022
Severity: CRITICAL
Description: Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Word 2013 SP1, Word 2013 RT SP1, Word 2016, Word for Mac 2011, Word 2016 for Mac, Office Compatibility Pack SP3, Word Viewer, Word Automation Services on SharePoint Server 2013 SP1, Office Web Apps Server 2013 SP1, and SharePoint Server 2013 SP1 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0052.

CVE ID: CVE-2016-0025
Severity: CRITICAL
Description: Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Word 2013 SP1, Word 2013 RT SP1, Office 2016, Word 2016, Word for Mac 2011, Word 2016 for Mac, Office Compatibility Pack SP3, Word Automation Services on SharePoint Server 2010 SP2, Word Automation Services on SharePoint Server 2013 SP1, Office Web Apps 2010 SP2, Office Web Apps Server 2013 SP1, and Office Online Server allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."

CVE ID: CVE-2016-0052
Severity: CRITICAL
Description: Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Word 2013 SP1, Word 2013 RT SP1, Word 2016, Word for Mac 2011, Word 2016 for Mac, Office Compatibility Pack SP3, Word Viewer, Word Automation Services on SharePoint Server 2013 SP1, Office Web Apps Server 2013 SP1, and SharePoint Server 2013 SP1 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0022.

CVE ID: CVE-2016-0053
Severity: CRITICAL
Description: Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Word 2013 SP1, Word 2013 RT SP1, Word 2016, Office Compatibility Pack SP3, Word Viewer, Word Automation Services on SharePoint Server 2013 SP1, Office Web Apps Server 2013 SP1, and SharePoint Server 2013 SP1 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."

CVE ID: CVE-2016-0056
Severity: CRITICAL
Description: Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Word 2013 SP1, Word 2013 RT SP1, Word 2016, and Office Compatibility Pack SP3 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."

CVE ID: CVE-2016-0127
Severity: CRITICAL
Description: Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Word 2013 SP1, Word 2013 RT SP1, Office Compatibility Pack SP3, Word Viewer, Word Automation Services on SharePoint Server 2010 SP2, Word Automation Services on SharePoint Server 2013 SP1, Office Web Apps 2010 SP2, and Office Web Apps Server 2013 SP1 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."

CVE ID: CVE-2016-0134
Severity: CRITICAL
Description: Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Word 2013 SP1, Word 2013 RT SP1, Word 2016, Word for Mac 2011, Word 2016 for Mac, Office Compatibility Pack SP3, Word Viewer, Word Automation Services on SharePoint Server 2010 SP2 and 2013 SP1, Office Web Apps 2010 SP2, and Web Apps Server 2013 SP1 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."

CVE ID: CVE-2016-0198
Severity: CRITICAL
Description: Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Word 2013 SP1, Word 2013 RT SP1, Word 2016, Word for Mac 2011, Word 2016 for Mac, Office Compatibility Pack SP3, and Word Viewer allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."

CVE ID: CVE-2016-3234
Severity: MODERATE
Description: Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Office Compatibility Pack SP3, Word Viewer, Word Automation Services on SharePoint Server 2010 SP2, Word Automation Services on SharePoint Server 2013 SP1, Office Web Apps 2010 SP2, and Office Web Apps Server 2013 SP1 allow remote attackers to obtain sensitive information from process memory via a crafted Office document, aka "Microsoft Office Information Disclosure Vulnerability."

CVE ID: CVE-2016-3280
Severity: CRITICAL
Description: Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Word 2013 SP1, Word 2013 RT SP1, Word for Mac 2011, Word 2016 for Mac, Office Compatibility Pack SP3, and Word Viewer allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."

CVE ID: CVE-2016-3282
Severity: CRITICAL
Description: Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Word 2013 SP1, Word 2013 RT SP1, Word 2016, Word for Mac 2011, Word 2016 for Mac, Office Compatibility Pack SP3, Word Viewer, Word Automation Services on SharePoint Server 2010 SP2, Word Automation Services on SharePoint Server 2013 SP1, SharePoint Server 2016, Office Web Apps 2010 SP2, Office Web Apps Server 2013 SP1, and Office Online Server allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."

CVE ID: CVE-2016-3317
Severity: CRITICAL
Description: Microsoft Office 2010 SP2, Word 2007 SP3, Word 2010 SP2, Word for Mac 2011, Word 2016 for Mac, and Word Viewer allow remote attackers to execute arbitrary code via a crafted file, aka "Microsoft Office Memory Corruption Vulnerability."

CVE ID: CVE-2016-7268
Severity: MODERATE
Description: Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Office Compatibility Pack SP3, Word Viewer, Word for Mac 2011, Word Automation Services on SharePoint Server 2010 SP2, and Office Web Apps 2010 SP2 allow remote attackers to obtain sensitive information from process memory or cause a denial of service (out-of-bounds read) via a crafted document, aka "Microsoft Office Information Disclosure Vulnerability."

CVE ID: CVE-2016-7290
Severity: MODERATE
Description: Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Office Compatibility Pack SP3, Word for Mac 2011, Word Automation Services on SharePoint Server 2010 SP2, and Office Web Apps 2010 SP2 allow remote attackers to obtain sensitive information from process memory or cause a denial of service (out-of-bounds read) via a crafted document, aka "Microsoft Office Information Disclosure Vulnerability," a different vulnerability than CVE-2016-7291.

CVE ID: CVE-2016-7291
Severity: MODERATE
Description: Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Office Compatibility Pack SP3, Word for Mac 2011, Word Automation Services on SharePoint Server 2010 SP2, and Office Web Apps 2010 SP2 allow remote attackers to obtain sensitive information from process memory or cause a denial of service (out-of-bounds read) via a crafted document, aka "Microsoft Office Information Disclosure Vulnerability," a different vulnerability than CVE-2016-7290.

CVE ID: CVE-2017-0031
Severity: CRITICAL
Description: Microsoft Office 2010 SP2, Office Compatibility Pack SP3, Word 2007 SP3, and Word 2010 SP2 allow r emote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted document, aka "Microsoft Office Memory Corruption Vulnerability." This vulnerability is different from tho se described in CVE-2017-0006, CVE-2017-0019, CVE-2017-0020, CVE-2017-0030, CVE-2017-0052, and CVE-2017-0053.

CVE ID: CVE-2017-0030
Severity: CRITICAL
Description: Microsoft Office 2010 SP2, Office Compatibility Pack SP3, Office Web Apps Server 2010 SP2, Word 20 07 SP3, Word 2010 SP2, and Word Automation Services on SharePoint Server 2010 SP2 allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted docum ent, aka "Microsoft Office Memory Corruption Vulnerability." This vulnerability is different from those des cribed in CVE-2017-0006, CVE-2017-0019, CVE-2017-0020, CVE-2017-0031, CVE-2017-0052, and CV E-2017-0053.

CVE ID: CVE-2017-0053
Severity: CRITICAL
Description: Microsoft Office 2010 SP2, Office Compatibility Pack SP3, Word 2007 SP3, Word 2010 SP2, Word 201 3 SP1, Word 2013 R2 SP1, Word 2016, and Word Viewer allow remote attackers to execute arbitrary co de or cause a denial of service (memory corruption) via a crafted document, aka "Microsoft Office Memo ry Corruption Vulnerability." This vulnerability is different from those described in CVE-2017-0006, CVE-2017-0019, CVE-2017-0020, CVE-2017-0030, CVE-2017-0031, and CVE-2017-0052.

CVE ID: CVE-2017-0105
Severity: MODERATE
Description: Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Word for Mac 2011, Office Compatibility Pack SP3, Word Automation Services on SharePoint Server 2010 SP2, and Office Web Apps 2010 SP2 allow remote attackers to obtain sensitive information from out-of-bound memory via a crafted Office do cument, aka "Microsoft Office Information Disclosure Vulnerability."

Windows Security Health Agent 6.1.7600.16385 (update available)
No vulnerabilities found.

Windows Media Player 12.0.7600.16385 (update available)
CVE ID: CVE-2010-2745
Severity: CRITICAL
Description: Microsoft Windows Media Player (WMP) 9 through 12 does not properly deallocate objects during a bro wser reload action, which allows user-assisted remote attackers to execute arbitrary code via crafted me dia content referenced in an HTML document, aka "Windows Media Player Memory Corruption Vulnera bility."

CVE ID: CVE-2015-1728
Severity: CRITICAL
Description: Microsoft Windows Media Player 10 through 12 allows remote attackers to execute arbitrary code via a crafted DataObject on a web site, aka "Windows Media Player RCE via DataObject Vulnerability."

CVE ID: CVE-2013-3127
Severity: CRITICAL
Description: The Microsoft WMV video codec in wmv9vcm.dll, wmvdmod.dll in Windows Media Format Runtime 9 a nd 9.5, and wmvdecod.dll in Windows Media Format Runtime 11 and Windows Media Player 11 and 12 allows remote attackers to execute arbitrary code via a crafted media file, aka "WMV Video Decoder Re mote Code Execution Vulnerability."

PSPad editor 4.5.5 (latest version)
No vulnerabilities found.

ESET Endpoint Security 5.0.2126.0 (update available)

No vulnerabilities found.

Notepad 6.1.7600.16385 (update available)
No vulnerabilities found.

Paint 6.1.7600.16385 (update available)
No vulnerabilities found.

Windows Firewall 6.1.7600.16385 (update available)
No vulnerabilities found.

DAEMON Tools Lite 4.45.4.0315 (update available)
No vulnerabilities found.

Google Chrome 58.0.3029.110 (update available)
No vulnerabilities found.

Mozilla Firefox 41.0.1 (update available)
No vulnerabilities found.

Windows Defender 6.1.7600.16385 (latest version)
No vulnerabilities found.

Zoner Photo Studio 14.0.1.2 (update available)
No vulnerabilities found.

Windows Backup and Restore 6.1.7600.16385 (update available)
No vulnerabilities found.

Compliance

ANTIMALWARE
ESET Endpoint Security
Last Scan Time: 03/29/2017 08:01 AM
Real Time Protection: Enabled
Virus Definition Database: Up-to-date
Antimalware Last Updated at: 06/15/2017 08:44 AM
Antimalware Version: 15586 (20170615)

Windows Defender
Last Scan Time: 06/14/2017 10:31 AM
Real Time Protection: Enabled
Virus Definition Database: Not Up-to-date
Antisypware Last Updated at: 05/10/2017 11:36 AM
Antisypware Version: 1.219.1406.0

BACKUP & CLOUD STORAGE
Windows Backup and Restore
Application State: Not Running
Last Backup Activity: No Backup Performed

ENCRYPTION
PASSWORD PROTECTION
Device is not password protected
CPU: Intel(R) Pentium(R) CPU G620 @ 2.60GHz
Device Identity: 0300020004000500000600700080009
Device Manufacturer: Gigabyte Tecohnology Co., Ltd.
Disk Space: Free Space 407.31GB Total Space 465.48GB
Is Device Virtual: False
Memory: Size 3.96GB Speed 1067 Mhz
Operating System: Microsoft Windows 7 Home Premium