微软发布 10 月补丁修复 61 个安全问题

安全威胁通告

发布时间：2019 年 10 月 9 日

综述

微软于周二发布了 10 月安全更新补丁，修复了 61 个从简单的欺骗攻击到远程执行代码的安全问题，产品涉及 Azure、Internet Explorer、Microsoft Browsers、Microsoft Devices、Microsoft Dynamics、Microsoft Edge、Microsoft Graphics Component、Microsoft JET Database Engine、Microsoft Office、Microsoft Office SharePoint、Microsoft Scripting Engine、Microsoft Windows、Open Source Software、Secure Boot、Servicing Stack Updates、SQL Server、Windows Hyper-V、Windows IIS、Windows Installer、Windows Kernel、Windows NTLM、Windows RDP 以及 Windows Update Stack。

相关信息如下：

产品	CVE 编号	CVE 标题	严重程度
Azure	CVE-2019-1372	Azure App Service 远程代码执行漏洞	Critical
Internet Explorer	CVE-2019-1371	Internet Explorer 内存破坏漏洞	Important
Microsoft Browsers	CVE-2019-0608	Microsoft Browser 欺骗漏洞	Important
Microsoft Browsers	CVE-2019-1357	Microsoft Browser 欺骗漏洞	Important
Microsoft Devices	CVE-2019-1314	Windows 10 Mobile 安全功能绕过漏洞	Important

Microsoft Dynamics	CVE-2019-1375	Microsoft Dynamics 365 (On-Premise) Cross Site Scripting Vulnerability	Important
Microsoft Edge	CVE-2019-1356	Microsoft Edge based on Edge HTML 信息泄露漏洞	Important
Microsoft Graphics Component	CVE-2019-1361	Microsoft Graphics Components 信息泄露漏洞	Important
Microsoft Graphics Component	CVE-2019-1362	Win32k 特权提升漏洞	Important
Microsoft Graphics Component	CVE-2019-1363	Windows GDI 信息泄露漏洞	Important
Microsoft Graphics Component	CVE-2019-1364	Win32k 特权提升漏洞	Important
Microsoft JET Database Engine	CVE-2019-1358	Jet Database Engine 远程代码执行漏洞	Important

Microsoft JET Database Engine	CVE-2019-1359	Jet Database Engine 远程代码执行漏洞	Important
Microsoft Office	CVE-2019-1327	Microsoft Excel 远程代码执行漏洞	Important
Microsoft Office	CVE-2019-1331	Microsoft Excel 远程代码执行漏洞	Important
Microsoft Office SharePoint	CVE-2019-1070	Microsoft Office SharePoint XSS Vulnerability	Important
Microsoft Office SharePoint	CVE-2019-1328	Microsoft SharePoint 欺骗漏洞	Important
Microsoft Office SharePoint	CVE-2019-1329	Microsoft SharePoint 特权提升漏洞	Important

Microsoft Office SharePoint	CVE-2019-1330	Microsoft SharePoint 特权提升漏洞	Important
Microsoft Scripting Engine	CVE-2019-1060	MS XML 远程代码执行漏洞	Critical
Microsoft Scripting Engine	CVE-2019-1307	Chakra Scripting Engine 内存破坏漏洞	Critical
Microsoft Scripting Engine	CVE-2019-1308	Chakra Scripting Engine 内存破坏漏洞	Critical
Microsoft Scripting Engine	CVE-2019-1238	VBScript 远程代码执行漏洞	Critical
Microsoft Scripting Engine	CVE-2019-1239	VBScript 远程代码执行漏洞	Critical

Microsoft Scripting Engine	CVE-2019-1335	Chakra Scripting Engine 内存破坏漏洞	Critical
Microsoft Scripting Engine	CVE-2019-1366	Chakra Scripting Engine 内存破坏漏洞	Critical
Microsoft Windows	CVE-2019-1341	Windows Power Service 特权提升漏洞	Important
Microsoft Windows	CVE-2019-1342	Windows Error Reporting Manager 特权提升漏洞	Important
Microsoft Windows	CVE-2019-1344	Windows Code Integrity Module 信息泄露漏洞	Important
Microsoft Windows	CVE-2019-1346	Windows 拒绝服务漏洞	Important

Microsoft Windows	CVE-2019-1347	Windows 拒绝服务漏洞	Important
Microsoft Windows	CVE-2019-1311	Windows Imaging API 远程代码执行漏洞	Important
Microsoft Windows	CVE-2019-1315	Windows Error Reporting Manager 特权提升漏洞	Important
Microsoft Windows	CVE-2019-1316	Microsoft Windows Setup 特权提升漏洞	Important
Microsoft Windows	CVE-2019-1317	Microsoft Windows 拒绝服务漏洞	Important
Microsoft Windows	CVE-2019-1318	Microsoft Windows Transport Layer Security 欺骗漏洞	Important

Microsoft Windows	CVE-2019-1319	Windows Error Reporting 特权提升漏洞	Important
Microsoft Windows	CVE-2019-1320	Microsoft Windows 特权提升漏洞	Important
Microsoft Windows	CVE-2019-1321	Microsoft Windows CloudStore 特权提升漏洞	Important
Microsoft Windows	CVE-2019-1322	Microsoft Windows 特权提升漏洞	Important
Microsoft Windows	CVE-2019-1325	Windows Redirected Drive Buffering System 特权提升漏洞	Moderate
Microsoft Windows	CVE-2019-1338	Windows NTLM 安全功能绕过漏洞	Important

Microsoft Windows	CVE-2019-1339	Windows Error Reporting Manager 特权提升漏洞	Important
Microsoft Windows	CVE-2019-1340	Microsoft Windows 特权提升漏洞	Important
Open Source Software	CVE-2019-1369	Open Enclave SDK 信息泄露漏洞	Important
Secure Boot	CVE-2019-1368	Windows Secure Boot 安全功能绕过漏洞	Important
Servicing Stack Updates	ADV990001	Latest Servicing Stack Updates	Critical
SQL Server	CVE-2019-1313	SQL Server Management Studio 信息泄露漏洞	Important
SQL Server	CVE-2019-1376	SQL Server Management Studio 信息泄露漏洞	Important

Windows Hyper-V	CVE-2019-1230	Hyper-V 信息泄露漏洞	Important
Windows IIS	CVE-2019-1365	Microsoft IIS Server 特权提升漏洞	Important
Windows Installer	CVE-2019-1378	Windows 10 Update Assistant 特权提升漏洞	Important
Windows Kernel	CVE-2019-1343	Windows 拒绝服务漏洞	Important
Windows Kernel	CVE-2019-1345	Windows Kernel 信息泄露漏洞	Important
Windows Kernel	CVE-2019-1334	Windows Kernel 信息泄露漏洞	Important
Windows NTLM	CVE-2019-1166	Windows NTLM Tampering Vulnerability	Important

Windows RDP	CVE-2019-1326	Windows Remote Desktop Protocol (RDP) 拒绝服务漏洞	Important
Windows RDP	CVE-2019-1333	Remote Desktop Client 远程代码执行漏洞	Critical
Windows Update Stack	CVE-2019-1323	Microsoft Windows Update Client 特权提升漏洞	Important
Windows Update Stack	CVE-2019-1336	Microsoft Windows Update Client 特权提升漏洞	Important
Windows Update Stack	CVE-2019-1337	Windows Update Client 信息泄露漏洞	Important

修复建议

微软官方已经发布更新补丁，请及时进行补丁更新。

附件

ADV990001 - Latest Servicing Stack Updates

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
ADV990001 MITRE NVD	**CVE Title:** Latest Servicing Stack Updates **Description:** This is a list of the latest servicing stack updates for each operating system. This list will be updated whenever a new servicing stack update is released. It is important to install the latest servicing stack update.	Critical	Defense in Depth

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: **1. Why are all of the Servicing Stack Updates (SSU) critical updates?** The SSUs are classified as Critical updates. This does not indicate that there is a critical vulnerability being addressed in the update. **2. When was the most recent SSU released for each version of Microsoft Windows?** Please refer to the following table for the most recent SSU release. We will update the entries any time a new SSU is released:		

Product	SSU Package	Date Released
Windows Server 2008	4517134	September 2019
Windows 7/Server 2008 R2	4516655	September 2019
Windows Server 2012	4521857	October 2019
Windows 8.1/Server 2012 R2	4521864	October 2019
Windows 10	4521856	October 2019
Windows 10 Version 1607/Server 2016	4521858	October 2019
Windows 10 Version 1703	4521859	October 2019
Windows 10 1709	4521860	October 2019

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Windows 10 1803/Windows Server, version 1803 4521861 October 2019 Windows 10 1809/Server 2019 4521862 October 2019 Windows 10 1903/Windows Server, version 1903 4521863 October 2019 **Mitigations:** None **Workarounds:** None **Revision:** 7.0 04/09/2019 07:00:00 A Servicing Stack Update has been released for Windows Server 2008 and Windows Server 2008 (Server Core installation); Windows 10 version 1809, Windows Server 2019, and Windows Server 2019 (Server Core installation). See the FAQ section for more information. 5.0 02/12/2019 08:00:00 A Servicing Stack Update has been released for Windows 10 Version 1607, Windows Server 2016, and Windows Server 2016 (Server Core installation); Windows 10 Version 1703; Windows 10 Version 1709 and Windows Server, version 1709 (Server Core		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Installation); Windows 10 Version 1803, and Windows Server, version 1803 (Server Core Installation). See the FAQ section for more information. 11.0 07/09/2019 07:00:00 A Servicing Stack Update has been released for all supported versions of Windows 10 (including Windows Server 2016 and 2019), Windows 8.1, Windows Server 2012 R2 and Windows Server 2012. See the FAQ section for more information. 5.2 02/14/2019 08:00:00 In the Security Updates table, corrected the Servicing Stack Update (SSU) for Windows 10 Version 1803 for x64-based Systems to 4485449. This is an informational change only. 12.0 07/24/2019 07:00:00 A Servicing Stack Update has been released for Windows 10 Version 1809 and Windows Server 2019. See the FAQ section for more information. 3.0 12/11/2018 08:00:00 A Servicing Stack Update has been released for Windows 10 Version 1709, Windows Server, version 1709 (Server Core Installation), Windows 10 Version 1803, and Windows Server, version 1803 (Server Core Installation). See the FAQ section for more information. 6.0 03/12/2019 07:00:00		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	A Servicing Stack Update has been released for Windows 7 and Windows Server 2008 R2 and Windows Server 2008 R2 (Server Core installation). See the FAQ section for more information. 9.0 06/11/2019 07:00:00 A Servicing Stack Update has been released for Windows 10 version 1607, Windows Server 2016, Windows 10 version 1809, and Windows Server 2019. See the FAQ section for more information. 8.0 05/14/2019 07:00:00 A Servicing Stack Update has been released for Windows 10 version 1507, Windows 10 version 1607, Windows Server 2016, Windows 10 version 1703, Windows 10 version 1709, Windows Server, version 1709, Windows 10 version 1803, Windows Server, version 1803, Windows 10 version 1809, Windows Server 2019, Windows 10 version 1809 and Windows Server, version 1809. See the FAQ section for more information. 4.0 01/08/2019 08:00:00 A Servicing Stack Update has been released for Windows 10 Version 1703. See the FAQ section for more information. 15.0 10/08/2019 07:00:00		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	A Servicing Stack Update has been released for all supported versions of Windows 10 (including Windows Server 2016 and 2019), Windows 8.1, Windows Server 2012 R2 and Windows Server 2012. See the FAQ section for more information. 14.0 09/10/2019 07:00:00 A Servicing Stack Update has been released for all supported versions of Windows. See the FAQ section for more information. 3.1 12/11/2018 08:00:00 Updated supersedence information. This is an informational change only. 3.2 12/12/2018 08:00:00 Fixed a typo in the FAQ. 1.1 11/14/2018 08:00:00 Corrected the link to the Windows Server 2008 Servicing Stack Update. This is an informational change only. 1.0 11/13/2018 08:00:00 Information published. 2.0 12/05/2018 08:00:00 A Servicing Stack Update has been released for Windows 10 Version 1809 and Windows Server 2019. See the FAQ section for more information.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	1.2 12/03/2018 08:00:00 FAQs have been added to further explain Security Stack Updates. The FAQs include a table that indicates the most recent SSU release for each Windows version. This is an informational change only. 13.0 07/26/2019 07:00:00 A Servicing Stack Update has been released for Windows 10 version 1903 and Windows Server, version 1903 (Server Core installation). See the FAQ section for more information. 5.1 02/13/2019 08:00:00 In the Security Updates table, corrected the Servicing Stack Update (SSU) for Windows 10 Version 1809 for x64-based Systems to 4470788. This is an informational change only. 10.0 06/14/2019 07:00:00 A Servicing Stack Update has been released for Windows 10 version 1903 and Windows Server, version 1903 (Server Core installation). See the FAQ section for more information.		

Affected Software

The following tables list the affected software details for the vulnerability.

ADV990001						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4516655 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 7 for x64-based Systems Service Pack 1	4516655 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4516655 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4516655 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes

ADV990001						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4516655 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4517134 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2012	4512939 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2012 (Server Core installation)	4512939 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 8.1 for 32-bit systems	4512938 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 8.1 for x64-based systems	4512938 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal:	Yes

ADV990001						
					N/A Vector: N/A	
Windows Server 2012 R2	4512938 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2012 R2 (Server Core installation)	4512938 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 for 32-bit Systems	4521856 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 for x64-based Systems	4521856 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2016	4521858 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes

ADV990001						
Windows 10 Version 1607 for 32-bit Systems	4521858 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1607 for x64-based Systems	4521858 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2016 (Server Core installation)	4521858 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1703 for 32-bit Systems	4521859 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1703 for x64-based Systems	4521859 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1709 for 32-bit Systems	4521860 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal:	Yes

ADV990001						
					N/A Vector: N/A	
Windows 10 Version 1709 for x64-based Systems	4521860 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1803 for 32-bit Systems	4521861 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1803 for x64-based Systems	4521861 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server, version 1803 (Server Core Installation)	4521861 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1803 for ARM64-based Systems	4521861 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes

ADV990001						
Windows 10 Version 1809 for 32-bit Systems	4521862 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1809 for x64-based Systems	4521862 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1809 for ARM64-based Systems	4521862 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2019	4521862 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2019 (Server Core installation)	4521862 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1709 for ARM64-based Systems	4521860 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal:	Yes

ADV990001						
					N/A Vector: N/A	
Windows 10 Version 1903 for 32-bit Systems	4521863 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1903 for x64-based Systems	4521863 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1903 for ARM64-based Systems	4521863 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server, version 1903 (Server Core installation)	4521863 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4517134 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes

ADV990001						
Windows Server 2008 for 32-bit Systems Service Pack 2	4517134 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4517134 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4517134 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0608 - Microsoft Browser Spoofing Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0608	**CVE Title:** Microsoft Browser Spoofing Vulnerability **Description:**	Important	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	A spoofing vulnerability exists when Microsoft Browsers does not properly parse HTTP content. An attacker who successfully exploited this vulnerability could impersonate a user request by crafting HTTP queries. The specially crafted website could either spoof content or serve as a pivot to chain an attack with other vulnerabilities in web services. To exploit the vulnerability, the user must click a specially crafted URL. In an email attack scenario, an attacker could send an email message containing the specially crafted URL to the user in an attempt to convince the user to click it. In a web-based attack scenario, an attacker could host a specially crafted website designed to appear as a legitimate website to the user. However, the attacker would have no way to force the user to visit the specially crafted website. The attacker would have to convince the user to visit the specially crafted website, typically by way of enticement in an email or instant message, and then convince the user to interact with content on the website. The update addresses the vulnerability by correcting how Microsoft Browsers parses HTTP responses. **FAQ:** None **Mitigations:** None		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Workarounds: None **Revision:** 1.0 10/08/2019 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-0608						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 9 on Windows	4519974 IE Cumulative 4520002	Low	Spoofing	4516026	Base: 2.4 Temporal: 2.2 Vector:	Yes

CVE-2019-0608						
Server 2008 for 32-bit Systems Service Pack 2	Monthly Rollup				CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2	4519974 IE Cumulative 4520002 Monthly Rollup	Low	Spoofing	4516026	Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1	4519974 IE Cumulative 4519976 Monthly Rollup	Important	Spoofing	4524157	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0608						
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1	4519974 IE Cumulative 4519976 Monthly Rollup	Important	Spoofing	4524157	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4519974 IE Cumulative 4519976 Monthly Rollup	Low	Spoofing	4524157	Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on	4519974 IE Cumulative	Low	Spoofing	4524135	Base: 2.4 Temporal: 2.2 Vector:	Yes

CVE-2019-0608						
Windows Server 2012					CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4519974 IE Cumulative 4520005 Monthly Rollup	Important	Spoofing	4524156	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 8.1 for x64-based systems	4519974 IE Cumulative 4520005 Monthly Rollup	Important	Spoofing	4524156	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2012 R2	4519974 IE Cumulative 4520005 Monthly Rollup	Low	Spoofing	4524156	Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0608						
Internet Explorer 11 on Windows RT 8.1	4520005 Monthly Rollup	Important	Spoofing	4524156	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 for 32-bit Systems	4520011 Security Update	Important	Spoofing	4524153	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 for x64-based Systems	4520011 Security Update	Important	Spoofing	4524153	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2016	4519998 Security Update	Low	Spoofing	4524152	Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0608						
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems	4519998 Security Update	Important	Spoofing	4524152	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4519998 Security Update	Important	Spoofing	4524152	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems	4520010 Security Update	Important	Spoofing	4524151	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0608						
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems	4520010 Security Update	Important	Spoofing	4524151	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems	4520004 Security Update	Important	Spoofing	4524150	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems	4520004 Security Update	Important	Spoofing	4524150	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0608						
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems	4520008 Security Update	Important	Spoofing	4524149	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems	4520008 Security Update	Important	Spoofing	4524149	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1803 for ARM64-	4520008 Security Update	Important	Spoofing	4524149	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0608						
based Systems						
Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems	4519338 Security Update	Important	Spoofing	4524148	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems	4519338 Security Update	Important	Spoofing	4524148	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1809 for	4519338 Security Update	Important	Spoofing	4524148	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0608						
ARM64-based Systems						
Internet Explorer 11 on Windows Server 2019	4519338 Security Update	Low	Spoofing	4524148	Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1709 for ARM64-based Systems	4520004 Security Update	Important	Spoofing	4524150	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version	4517389 Security Update	Important	Spoofing	4524147	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0608						
1903 for 32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1903 for x64-based Systems	4517389 Security Update	Important	Spoofing	4524147	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1903 for ARM64-based Systems	4517389 Security Update	Important	Spoofing	4524147	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 10 on	4520007 Monthly Rollup 4519974 IE	Low	Spoofing	4524135	Base: 2.4 Temporal: 2.2 Vector:	Yes

CVE-2019-0608						
Windows Server 2012	Cumulative				CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	
Microsoft Edge (EdgeHTML-based) on Windows 10 for 32-bit Systems	4520011 Security Update	Important	Spoofing	4524153	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 for x64-based Systems	4520011 Security Update	Important	Spoofing	4524153	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on	4519998 Security Update	Low	Spoofing	4524152	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0608						
Windows Server 2016						
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1607 for 32-bit Systems	4519998 Security Update	Important	Spoofing	4524152	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1607 for x64-based Systems	4519998 Security Update	Important	Spoofing	4524152	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on	4520010 Security Update	Important	Spoofing	4524151	Base: 4.3 Temporal: 3.9 Vector:	Yes

CVE-2019-0608						
Windows 10 Version 1703 for 32-bit Systems					CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1703 for x64-based Systems	4520010 Security Update	Important	Spoofing	4524151	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1709 for 32-bit Systems	4520004 Security Update	Important	Spoofing	4524150	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge	4520004 Security	Important	Spoofing	4524150	Base: 4.3 Temporal: 3.9	Yes

CVE-2019-0608						
(EdgeHTML-based) on Windows 10 Version 1709 for x64-based Systems	Update				Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for 32-bit Systems	4520008 Security Update	Important	Spoofing	4524149	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for	4520008 Security Update	Important	Spoofing	4524149	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0608						
x64-based Systems						
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for ARM64-based Systems	4520008 Security Update	Important	Spoofing	4524149	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for 32-bit Systems	4519338 Security Update	Important	Spoofing	4524148	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML	4519338 Security	Important	Spoofing	4524148	Base: 4.3 Temporal: 3.9 Vector:	Yes

CVE-2019-0608						
-based) on Windows 10 Version 1809 for x64-based Systems	Update				CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for ARM64-based Systems	4519338 Security Update	Important	Spoofing	4524148	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows Server 2019	4519338 Security Update	Low	Spoofing	4524148	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0608						
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1709 for ARM64-based Systems	4520004 Security Update	Important	Spoofing	4524150	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for 32-bit Systems	4517389 Security Update	Important	Spoofing	4524147	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10	4517389 Security Update	Important	Spoofing	4524147	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0608						
Version 1903 for x64-based Systems						
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for ARM64-based Systems	4517389 Security Update	Important	Spoofing	4524147	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1060 - MS XML Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1060 MITRE NVD	**CVE Title:** MS XML Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input. An attacker who successfully exploited the vulnerability could run malicious code remotely to take control of the userâ€™s system. To exploit the vulnerability, an attacker could host a specially crafted website designed to invoke MSXML through a web browser. However, an attacker would have no way to force a user to visit such a website. Instead, an attacker would typically have to convince a user to either click a link in an email message or instant message that would then take the user to the website. When Internet Explorer parses the XML content, an attacker could run malicious code remotely to take control of the userâ€™s system. The update addresses the vulnerability by correcting how the MSXML parser processes user input. **FAQ:** None **Mitigations:**	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Workarounds:** None **Revision:** 1.0 10/08/2019 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1060						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows Server 2012	4519985 Security Only 4520007	Critical	Remote Code Execution	4524154	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1060						
	Monthly Rollup					
Windows Server 2012 (Server Core installation)	4519985 Security Only 4520007 Monthly Rollup	Critical	Remote Code Execution	4524154	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4519990 Security Only 4520005 Monthly Rollup	Critical	Remote Code Execution	4524156	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4519990 Security Only 4520005 Monthly	Critical	Remote Code Execution	4524156	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1060						
	Rollup					
Windows Server 2012 R2	4519990 Security Only 4520005 Monthly Rollup	Critical	Remote Code Execution	4524156	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4520005 Monthly Rollup	Critical	Remote Code Execution	4524156	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4519990 Security Only 4520005 Monthly Rollup	Critical	Remote Code Execution	4524156	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4520011 Security	Critical	Remote Code Execution	4524153	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-1060						
	Update					
Windows 10 for x64-based Systems	4520011 Security Update	Critical	Remote Code Execution	4524153	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2016	4519998 Security Update	Critical	Remote Code Execution	4524152	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1607 for 32-bit Systems	4519998 Security Update	Critical	Remote Code Execution	4524152	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1607 for x64-based Systems	4519998 Security Update	Critical	Remote Code Execution	4524152	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2016 (Server	4519998 Security	Critical	Remote Code Execution	4524152	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-1060						
Core installation)	Update					
Windows 10 Version 1703 for 32-bit Systems	4520010 Security Update	Critical	Remote Code Execution	4524151	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1703 for x64-based Systems	4520010 Security Update	Critical	Remote Code Execution	4524151	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1709 for 32-bit Systems	4520004 Security Update	Critical	Remote Code Execution	4524150	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1709 for x64-based Systems	4520004 Security Update	Critical	Remote Code Execution	4524150	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-1060						
Windows 10 Version 1803 for 32-bit Systems	4520008 Security Update	Critical	Remote Code Execution	4524149	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1803 for x64-based Systems	4520008 Security Update	Critical	Remote Code Execution	4524149	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server, version 1803 (Server Core Installation)	4520008 Security Update	Critical	Remote Code Execution	4524149	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1803 for ARM64-based Systems	4520008 Security Update	Critical	Remote Code Execution	4524149	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-1060						
Windows 10 Version 1809 for 32-bit Systems	4519338 Security Update	Critical	Remote Code Execution	4524148	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4519338 Security Update	Critical	Remote Code Execution	4524148	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4519338 Security Update	Critical	Remote Code Execution	4524148	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4519338 Security Update	Critical	Remote Code Execution	4524148	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server	4519338 Security	Critical	Remote Code Execution	4524148	Base: 6.4 Temporal: 5.8	Yes

CVE-2019-1060						
Core installation)	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1709 for ARM64-based Systems	4520004 Security Update	Critical	Remote Code Execution	4524150	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1903 for 32-bit Systems	4517389 Security Update	Critical	Remote Code Execution	4524147	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1903 for x64-based Systems	4517389 Security Update	Critical	Remote Code Execution	4524147	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1903 for ARM64-	4517389 Security Update	Critical	Remote Code Execution	4524147	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-1060						
based Systems						
Windows Server, version 1903 (Server Core installation)	4517389 Security Update	Critical	Remote Code Execution	4524147	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-1070 - Microsoft Office SharePoint XSS Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1070 MITRE NVD	**CVE Title:** Microsoft Office SharePoint XSS Vulnerability **Description:** A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server.	Important	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. The attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests. **FAQ:** **Is the Preview Pane an attack vector for this vulnerability?** No, the Preview Pane is not an attack vector. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/08/2019 07:00:00		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1070						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SharePoint Foundation 2013 Service Pack 1	4484122 Security Update	Important	Spoofing	4484098	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Enterprise Server 2016	4484111 Security Update	Important	Spoofing	4475590	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1166 - Windows NTLM Tampering Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1166 MITRE NVD	**CVE Title:** Windows NTLM Tampering Vulnerability **Description:** A tampering vulnerability exists in Microsoft Windows when a man-in-the-middle attacker is able to successfully bypass the NTLM MIC (Message Integrity Check) protection. An attacker who successfully exploited this vulnerability could gain the ability to downgrade NTLM security features. To exploit this vulnerability, the attacker would need to tamper with the NTLM exchange. The attacker could then modify flags of the NTLM packet without invalidating the signature. The update addresses the vulnerability by hardening NTLM MIC protection on the server-side. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Tampering

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 10/08/2019 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1166						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4520003 Security Only 451997	Important	Tampering	4524157	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1166						
	6 Monthly Rollup					
Windows 7 for x64-based Systems Service Pack 1	4519976 Monthly Rollup 4520003 Security Only	Important	Tampering	4524157	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core	4519976 Monthly Rollup 4520003 Security Only	Important	Tampering	4524157	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1166						
installation)						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4519976 Monthly Rollup 4520003 Security Only	Important	Tampering	4524157	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4519976 Monthly Rollup 4520003 Security Only	Important	Tampering	4524157	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for	4520002 Monthly	Important	Tampering	4516026	Base: 5.9 Temporal: 5.3 Vector:	Yes

CVE-2019-1166						
32-bit Systems Service Pack 2 (Server Core installation)	Rollup 4520009 Security Only				CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	
Windows Server 2012	4519985 Security Only 4520007 Monthly Rollup	Important	Tampering	4524154	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core	4519985 Security Only 4520007	Important	Tampering	4524154	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1166						
installation)	Monthly Rollup					
Windows 8.1 for 32-bit systems	4519990 Security Only 4520005 Monthly Rollup	Important	Tampering	4524156	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4519990 Security Only 4520005 Monthly Rollup	Important	Tampering	4524156	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1166						
Windows Server 2012 R2	4519990 Security Only 4520005 Monthly Rollup	Important	Tampering	4524156	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4520005 Monthly Rollup	Important	Tampering	4524156	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4519990 Security Only 4520005 Monthly Rollup	Important	Tampering	4524156	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1166						
Windows 10 for 32-bit Systems	4520011 Security Update	Important	Tampering	4524153	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4520011 Security Update	Important	Tampering	4524153	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4519998 Security Update	Important	Tampering	4524152	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4519998 Security Update	Important	Tampering	4524152	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for	4519998 Security	Important	Tampering	4524152	Base: 5.9 Temporal: 5.3 Vector:	Yes

CVE-2019-1166						
x64-based Systems	Update				CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	
Windows Server 2016 (Server Core installation)	4519998 Security Update	Important	Tampering	4524152	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4520010 Security Update	Important	Tampering	4524151	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4520010 Security Update	Important	Tampering	4524151	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for	4520004 Security	Important	Tampering	4524150	Base: 5.9 Temporal: 5.3 Vector:	Yes

CVE-2019-1166						
32-bit Systems	Update				CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1709 for x64-based Systems	4520004 Security Update	Important	Tampering	4524150	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4520008 Security Update	Important	Tampering	4524149	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4520008 Security Update	Important	Tampering	4524149	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core	4520008 Security Update	Important	Tampering	4524149	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1166						
Installation)						
Windows 10 Version 1803 for ARM64-based Systems	4520008 Security Update	Important	Tampering	4524149	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4519338 Security Update	Important	Tampering	4524148	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4519338 Security Update	Important	Tampering	4524148	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-	4519338 Security Update	Important	Tampering	4524148	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1166						
based Systems						
Windows Server 2019	4519338 Security Update	Important	Tampering	4524148	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4519338 Security Update	Important	Tampering	4524148	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4520004 Security Update	Important	Tampering	4524150	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for	4517389 Security	Important	Tampering	4524147	Base: 5.9 Temporal: 5.3 Vector:	Yes

CVE-2019-1166						
32-bit Systems	Update				CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1903 for x64-based Systems	4517389 Security Update	Important	Tampering	4524147	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4517389 Security Update	Important	Tampering	4524147	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4517389 Security Update	Important	Tampering	4524147	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server	4520002	Important	Tampering	4516026	Base: 5.9 Temporal: 5.3	Yes

CVE-2019-1166						
2008 for Itanium-Based Systems Service Pack 2	Monthly Rollup 4520009 Security Only				Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	
Windows Server 2008 for 32-bit Systems Service Pack 2	4520002 Monthly Rollup 4520009 Security Only	Important	Tampering	4516026	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4520002 Monthly Rollup 4520009 Security	Important	Tampering	4516026	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1166						
	Only					
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4520002 Monthly Rollup 4520009 Security Only	Important	Tampering	4516026	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1230 - Hyper-V Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-	**CVE Title:** Hyper-V Information Disclosure Vulnerability **Description:**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
1230 MITRE NVD	An information disclosure vulnerability exists when the Windows Hyper-V Network Switch on a host operating system fails to properly validate input from an authenticated user on a guest operating system. To exploit the vulnerability, an attacker on a guest operating system could run a specially crafted application that could cause the Hyper-V host operating system to disclose memory information. An attacker who successfully exploited the vulnerability could gain access to information on the Hyper-V host operating system. The security update addresses the vulnerability by correcting how the Windows Hyper-V Network Switch validates guest operating system user input. **FAQ:** **What type of information could be disclosed by this vulnerability?** The type of information that could be disclosed if an attacker successfully exploited this vulnerability is Guest VM to Hyper-V host server - virtualization security boundary. **Mitigations:** None **Workarounds:**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 10/08/2019 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1230						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1703 for x64-based Systems	4520010 Security Update	Important	Information Disclosure	4524151	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1230						
Windows 10 Version 1709 for x64-based Systems	4520004 Security Update	Important	Information Disclosure	4524150	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4520008 Security Update	Important	Information Disclosure	4524149	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4520008 Security Update	Important	Information Disclosure	4524149	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4519338 Security Update	Important	Information Disclosure	4524148	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1230						
Windows Server 2019	4519338 Security Update	Important	Information Disclosure	4524148	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4519338 Security Update	Important	Information Disclosure	4524148	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1238 - VBScript Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1238	**CVE Title:** VBScript Remote Code Execution Vulnerability **Description:**	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the IE rendering engine. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability. The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory. **FAQ:** None		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 10/08/2019 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1238						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 9 on	4519974 IE Cumulative 4520002	Moderate	Remote Code Execution	4516026	Base: 6.4 Temporal: 5.8	Yes

CVE-2019-1238						
Windows Server 2008 for 32-bit Systems Service Pack 2	Monthly Rollup				Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2	4519974 IE Cumulative 4520002 Monthly Rollup	Moderate	Remote Code Execution	4516026	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 7 for 32-	4519974 IE Cumulative 4519976 Monthly	Critical	Remote Code Execution	4524157	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1238						
bit Systems Service Pack 1	Rollup					
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1	4519974 IE Cumulative 4519976 Monthly Rollup	Critical	Remote Code Execution	4524157	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems	4519974 IE Cumulative 4519976 Monthly Rollup	Moderate	Remote Code Execution	4524157	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1238						
Service Pack 1						
Internet Explorer 11 on Windows Server 2012	4519974 IE Cumulative	Moderate	Remote Code Execution	4524135	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4519974 IE Cumulative 4520005 Monthly Rollup	Critical	Remote Code Execution	4524156	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 8.1 for x64-based systems	4519974 IE Cumulative 4520005 Monthly Rollup	Critical	Remote Code Execution	4524156	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1238						
Internet Explorer 11 on Windows Server 2012 R2	4519974 IE Cumulative 4520005 Monthly Rollup	Moderate	Remote Code Execution	4524156	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows RT 8.1	4520005 Monthly Rollup	Critical	Remote Code Execution	4524156	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 for 32-bit Systems	4520011 Security Update	Critical	Remote Code Execution	4524153	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 for	4520011 Security Update	Critical	Remote Code Execution	4524153	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1238						
x64-based Systems						
Internet Explorer 11 on Windows Server 2016	4519998 Security Update	Moderate	Remote Code Execution	4524152	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems	4519998 Security Update	Critical	Remote Code Execution	4524152	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10	4519998 Security Update	Critical	Remote Code Execution	4524152	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1238						
Version 1607 for x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems	4520010 Security Update	Critical	Remote Code Execution	4524151	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1703 for x64-	4520010 Security Update	Critical	Remote Code Execution	4524151	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1238						
based Systems						
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems	4520004 Security Update	Critical	Remote Code Execution	4524150	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems	4520004 Security Update	Critical	Remote Code Execution	4524150	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1238						
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems	4520008 Security Update	Critical	Remote Code Execution	4524149	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems	4520008 Security Update	Critical	Remote Code Execution	4524149	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows	4520008 Security Update	Critical	Remote Code Execution	4524149	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1238						
10 Version 1803 for ARM64-based Systems						
Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems	4519338 Security Update	Critical	Remote Code Execution	4524148	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1809 for x64-	4519338 Security Update	Critical	Remote Code Execution	4524148	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1238						
based Systems						
Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems	4519338 Security Update	Critical	Remote Code Execution	4524148	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2019	4519338 Security Update	Moderate	Remote Code Execution	4524148	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10	4520004 Security Update	Critical	Remote Code Execution	4524150	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1238						
Version 1709 for ARM64-based Systems						
Internet Explorer 11 on Windows 10 Version 1903 for 32-bit Systems	4517389 Security Update	Critical	Remote Code Execution	4524147	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1903 for x64-	4517389 Security Update	Critical	Remote Code Execution	4524147	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1238						
based Systems						
Internet Explorer 11 on Windows 10 Version 1903 for ARM64-based Systems	4517389 Security Update	Critical	Remote Code Execution	4524147	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 10 on Windows Server 2012	4520007 Monthly Rollup 4519974 IE Cumulative	Moderate	Remote Code Execution	4524135	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1239 - VBScript Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1239 MITRE NVD	**CVE Title:** VBScript Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the IE rendering engine. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/08/2019 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1239						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems	4519338 Security Update	Critical	Remote Code Execution	4524148	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems	4519338 Security Update	Critical	Remote Code Execution	4524148	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version	4519338 Security Update	Critical	Remote Code Execution	4524148	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1239						
1809 for ARM64-based Systems						
Internet Explorer 11 on Windows Server 2019	4519338 Security Update	Critical	Remote Code Execution	4524148	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1307 - Chakra Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1307	**CVE Title:** Chakra Scripting Engine Memory Corruption Vulnerability **Description:**	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability. The security update addresses the vulnerability by modifying how the Chakra scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Workarounds: None **Revision:** 1.0 10/08/2019 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1307						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge (EdgeHTML-based) on Windows 10	4520011 Security Update	Critical	Remote Code Execution	4524153	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1307						
for 32-bit Systems						
Microsoft Edge (EdgeHTML-based) on Windows 10 for x64-based Systems	4520011 Security Update	Critical	Remote Code Execution	4524153	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows Server 2016	4519998 Security Update	Moderate	Remote Code Execution	4524152	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version	4519998 Security Update	Critical	Remote Code Execution	4524152	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1307						
1607 for 32-bit Systems						
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1607 for x64-based Systems	4519998 Security Update	Critical	Remote Code Execution	4524152	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1703 for 32-bit Systems	4520010 Security Update	Critical	Remote Code Execution	4524151	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on	4520010 Security Update	Critical	Remote Code Execution	4524151	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1307						
Windows 10 Version 1703 for x64-based Systems						
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1709 for 32-bit Systems	4520004 Security Update	Critical	Remote Code Execution	4524150	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1709 for x64-based Systems	4520004 Security Update	Critical	Remote Code Execution	4524150	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1307						
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for 32-bit Systems	4520008 Security Update	Critical	Remote Code Execution	4524149	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for x64-based Systems	4520008 Security Update	Critical	Remote Code Execution	4524149	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version	4520008 Security Update	Critical	Remote Code Execution	4524149	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1307						
1803 for ARM64-based Systems						
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for 32-bit Systems	4519338 Security Update	Critical	Remote Code Execution	4524148	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for x64-based Systems	4519338 Security Update	Critical	Remote Code Execution	4524148	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1307						
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for ARM64-based Systems	4519338 Security Update	Critical	Remote Code Execution	4524148	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows Server 2019	4519338 Security Update	Moderate	Remote Code Execution	4524148	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1709 for	4520004 Security Update	Critical	Remote Code Execution	4524150	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1307						
ARM64-based Systems						
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for 32-bit Systems	4517389 Security Update	Critical	Remote Code Execution	4524147	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for x64-based Systems	4517389 Security Update	Critical	Remote Code Execution	4524147	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-	4517389 Security	Critical	Remote Code Execution	4524147	Base: 4.2 Temporal: 3.8	Yes

CVE-2019-1307						
based) on Windows 10 Version 1903 for ARM64-based Systems	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
ChakraCore	Release Notes Security Update	Critical	Remote Code Execution	4524147	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1308 - Chakra Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1308 MITRE NVD	**CVE Title:** Chakra Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by modifying how the Chakra scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/08/2019 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1308						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge (EdgeHTML-based) on Windows 10 for 32-bit Systems	4520011 Security Update	Critical	Remote Code Execution	4524153	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 for x64-based Systems	4520011 Security Update	Critical	Remote Code Execution	4524153	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows Server 2016	4519998 Security Update	Moderate	Remote Code Execution	4524152	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1308						
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1607 for 32-bit Systems	4519998 Security Update	Critical	Remote Code Execution	4524152	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1607 for x64-based Systems	4519998 Security Update	Critical	Remote Code Execution	4524152	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version	4520010 Security Update	Critical	Remote Code Execution	4524151	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1308						
1703 for 32-bit Systems						
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1703 for x64-based Systems	4520010 Security Update	Critical	Remote Code Execution	4524151	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1709 for 32-bit Systems	4520004 Security Update	Critical	Remote Code Execution	4524150	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on	4520004 Security Update	Critical	Remote Code Execution	4524150	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1308						
Windows 10 Version 1709 for x64-based Systems						
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for 32-bit Systems	4520008 Security Update	Critical	Remote Code Execution	4524149	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for x64-based Systems	4520008 Security Update	Critical	Remote Code Execution	4524149	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1308						
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for ARM64-based Systems	4520008 Security Update	Critical	Remote Code Execution	4524149	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for 32-bit Systems	4519338 Security Update	Critical	Remote Code Execution	4524148	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10	4519338 Security Update	Critical	Remote Code Execution	4524148	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1308						
Version 1809 for x64-based Systems						
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for ARM64-based Systems	4519338 Security Update	Critical	Remote Code Execution	4524148	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows Server 2019	4519338 Security Update	Moderate	Remote Code Execution	4524148	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-	4520004 Security	Critical	Remote Code Execution	4524150	Base: 4.2 Temporal: 3.8	Yes

CVE-2019-1308						
based) on Windows 10 Version 1709 for ARM64-based Systems	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for 32-bit Systems	4517389 Security Update	Critical	Remote Code Execution	4524147	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for	4517389 Security Update	Critical	Remote Code Execution	4524147	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1308						
x64-based Systems						
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for ARM64-based Systems	4517389 Security Update	Critical	Remote Code Execution	4524147	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
ChakraCore	Release Notes Security Update	Critical	Remote Code Execution	4524147	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Maybe

CVE-2019-1311 - Windows Imaging API Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1311 MITRE NVD	**CVE Title:** Windows Imaging API Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when the Windows Imaging API improperly handles objects in memory. The vulnerability could corrupt memory in a way that enables an attacker to execute arbitrary code in the context of the current user. To exploit the vulnerability, an attacker would have to convince a user to open a specially crafted .WIM file. The update addresses the vulnerability by modifying how the WIM service handles objects in memory. **FAQ:** None **Mitigations:**	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Workarounds:** None **Revision:** 1.0 10/08/2019 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1311						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows Server 2012	4519985 Security Only 4520007	Important	Remote Code Execution	4524154	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1311						
	Monthly Rollup					
Windows Server 2012 (Server Core installation)	4519985 Security Only 4520007 Monthly Rollup	Important	Remote Code Execution	4524154	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4519990 Security Only 4520005 Monthly Rollup	Important	Remote Code Execution	4524156	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4519990 Security Only 4520005 Monthly	Important	Remote Code Execution	4524156	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1311						
	Rollup					
Windows Server 2012 R2	4519990 Security Only 4520005 Monthly Rollup	Important	Remote Code Execution	4524156	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4520005 Monthly Rollup	Important	Remote Code Execution	4524156	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4519990 Security Only 4520005 Monthly Rollup	Important	Remote Code Execution	4524156	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4520011 Security	Important	Remote Code Execution	4524153	Base: 7.8 Temporal: 7	Yes

CVE-2019-1311						
	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 for x64-based Systems	4520011 Security Update	Important	Remote Code Execution	4524153	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4519998 Security Update	Important	Remote Code Execution	4524152	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4519998 Security Update	Important	Remote Code Execution	4524152	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4519998 Security Update	Important	Remote Code Execution	4524152	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server	4519998 Security	Important	Remote Code Execution	4524152	Base: 7.8 Temporal: 7	Yes

CVE-2019-1311						
Core installation)	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1703 for 32-bit Systems	4520010 Security Update	Important	Remote Code Execution	4524151	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4520010 Security Update	Important	Remote Code Execution	4524151	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4520004 Security Update	Important	Remote Code Execution	4524150	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4520004 Security Update	Important	Remote Code Execution	4524150	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1311						
Windows 10 Version 1803 for 32-bit Systems	4520008 Security Update	Important	Remote Code Execution	4524149	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4520008 Security Update	Important	Remote Code Execution	4524149	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4520008 Security Update	Important	Remote Code Execution	4524149	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4520008 Security Update	Important	Remote Code Execution	4524149	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1311						
Windows 10 Version 1809 for 32-bit Systems	4519338 Security Update	Important	Remote Code Execution	4524148	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4519338 Security Update	Important	Remote Code Execution	4524148	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4519338 Security Update	Important	Remote Code Execution	4524148	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4519338 Security Update	Important	Remote Code Execution	4524148	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server	4519338 Security	Important	Remote Code Execution	4524148	Base: 7.8 Temporal: 7	Yes

CVE-2019-1311						
Core installation)	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1709 for ARM64-based Systems	4520004 Security Update	Important	Remote Code Execution	4524150	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4517389 Security Update	Important	Remote Code Execution	4524147	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4517389 Security Update	Important	Remote Code Execution	4524147	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-	4517389 Security Update	Important	Remote Code Execution	4524147	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1311						
based Systems						
Windows Server, version 1903 (Server Core installation)	4517389 Security Update	Important	Remote Code Execution	4524147	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1313 - SQL Server Management Studio Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1313	**CVE Title:** SQL Server Management Studio Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists in Microsoft SQL Server Management Studio (SSMS) when it improperly enforces permissions. An attacker could exploit the	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	vulnerability if the attacker's credentials allow access to an affected SQL server database. An attacker who successfully exploited the vulnerability could gain additional database and file information. The security update addresses the vulnerability by correcting how SQL Server Management Studio enforces permissions. **FAQ:** **What type of information could be disclosed by this vulnerability?** The type of information that could be disclosed if an attacker successfully exploited this vulnerability relates to SQL table columns that would normally be restricted. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/08/2019 07:00:00		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1313						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
SQL Server Management Studio 18.3	Release Notes Security Update	Important	Information Disclosure		Base: N/A Temporal: N/A Vector: N/A	Maybe
SQL Server Management Studio 18.3.1	Release Notes Security Update	Important	Information Disclosure		Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1314 - Windows 10 Mobile Security Feature Bypass Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1314 MITRE NVD	**CVE Title:** Windows 10 Mobile Security Feature Bypass Vulnerability **Description:** A security feature bypass vulnerability exists in Windows 10 Mobile when Cortana allows a user to access files and folders through the locked screen. An attacker who successfully exploited this vulnerability could access the photo library of an affected phone and modify or delete photos without authenticating to the system. To exploit the vulnerability, an attacker would require physical access and the phone would need to have Cortana assistance allowed from the lock screen. **FAQ:** **Where do I find the update for Windows 10 Mobile?** Microsoft is not planning on fixing this vulnerability in Windows 10 Mobile. Microsoft recommends implementing the workaround to restrict access to Cortana.	Important	Security Feature Bypass

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** The following workaround can protect users from this vulnerability by disabling access to Cortana on the phone lock screen. This can be accomplished by following these steps: 1. Open the **Cortana** app from the applications screen. 2. Tap on the **Menu button** (3 horizontal bars) in the top left of the Cortana app. 3. Tap on **Settings** option. 4. Set the slider for the **Lock Screen** option to **Off** to prevent access to Cortana when the device is locked. **Revision:** 1.0 10/08/2019 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1314						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Mobile		Important	Security Feature Bypass		Base: N/A Temporal: N/A Vector: N/A	

CVE-2019-1315 - Windows Error Reporting Manager Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1315 MITRE NVD	**CVE Title:** Windows Error Reporting Manager Elevation of Privilege Vulnerability **Description:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	An elevation of privilege vulnerability exists when Windows Error Reporting manager improperly handles hard links. An attacker who successfully exploited this vulnerability could overwrite a targeted file leading to an elevated status. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. The security update addresses the vulnerability by correcting how Windows Error Reporting manager handles hard links. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/08/2019 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1315						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4520003 Security Only 4519976 Monthly Rollup	Important	Elevation of Privilege	4524157	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4519976 Monthly Rollup 4520003 Security Only	Important	Elevation of Privilege	4524157	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1315						
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4519976 Monthly Rollup 4520003 Security Only	Important	Elevation of Privilege	4524157	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4519976 Monthly Rollup 4520003 Security Only	Important	Elevation of Privilege	4524157	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems	4519976 Monthly Rollup 4520003 Security	Important	Elevation of Privilege	4524157	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1315						
Service Pack 1	Only					
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4520002 Monthly Rollup 4520009 Security Only	Important	Elevation of Privilege	4516026	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012	4519985 Security Only 4520007 Monthly Rollup	Important	Elevation of Privilege	4524154	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4519985 Security Only 4520007 Monthly	Important	Elevation of Privilege	4524154	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1315						
	Rollup					
Windows 8.1 for 32-bit systems	4519990 Security Only 4520005 Monthly Rollup	Important	Elevation of Privilege	4524156	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4519990 Security Only 4520005 Monthly Rollup	Important	Elevation of Privilege	4524156	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4519990 Security Only 4520005 Monthly Rollup	Important	Elevation of Privilege	4524156	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1315						
Windows RT 8.1	4520005 Monthly Rollup	Important	Elevation of Privilege	4524156	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4519990 Security Only 4520005 Monthly Rollup	Important	Elevation of Privilege	4524156	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4520011 Security Update	Important	Elevation of Privilege	4524153	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4520011 Security Update	Important	Elevation of Privilege	4524153	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4519998 Security Update	Important	Elevation of Privilege	4524152	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1315						
Windows 10 Version 1607 for 32-bit Systems	4519998 Security Update	Important	Elevation of Privilege	4524152	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4519998 Security Update	Important	Elevation of Privilege	4524152	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4519998 Security Update	Important	Elevation of Privilege	4524152	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4520010 Security Update	Important	Elevation of Privilege	4524151	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4520010 Security Update	Important	Elevation of Privilege	4524151	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1315						
Windows 10 Version 1709 for 32-bit Systems	4520004 Security Update	Important	Elevation of Privilege	4524150	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4520004 Security Update	Important	Elevation of Privilege	4524150	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4520008 Security Update	Important	Elevation of Privilege	4524149	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4520008 Security Update	Important	Elevation of Privilege	4524149	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server	4520008 Security Update	Important	Elevation of Privilege	4524149	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1315						
Core Installation)						
Windows 10 Version 1803 for ARM64-based Systems	4520008 Security Update	Important	Elevation of Privilege	4524149	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1315						
Windows Server 2019	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4520004 Security Update	Important	Elevation of Privilege	4524150	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4517389 Security Update	Important	Elevation of Privilege	4524147	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4517389 Security Update	Important	Elevation of Privilege	4524147	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1315						
Windows 10 Version 1903 for ARM64-based Systems	4517389 Security Update	Important	Elevation of Privilege	4524147	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4517389 Security Update	Important	Elevation of Privilege	4524147	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4520002 Monthly Rollup 4520009 Security Only	Important	Elevation of Privilege	4516026	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems	4520002 Monthly Rollup 4520009	Important	Elevation of Privilege	4516026	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1315						
Service Pack 2	Security Only					
Windows Server 2008 for x64-based Systems Service Pack 2	4520002 Monthly Rollup 4520009 Security Only	Important	Elevation of Privilege	4516026	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4520002 Monthly Rollup 4520009 Security Only	Important	Elevation of Privilege	4516026	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1316 - Microsoft Windows Setup Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1316 MITRE NVD	**CVE Title:** Microsoft Windows Setup Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in Microsoft Windows Setup when it does not properly handle privileges. An attacker who successfully exploited this vulnerability could run processes in an elevated context. An attacker could then install programs; view, change or delete data. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. The security update addresses the vulnerability by enabling Windows Setup to properly handle user privileges. **FAQ:** None	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 10/08/2019 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1316						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	4520011 Security	Important	Elevation of Privilege	4524153	Base: 7.3 Temporal: 6.6	Yes

CVE-2019-1316						
	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:H/A:N/E:P/RL:O/RC:C	
Windows 10 for x64-based Systems	4520011 Security Update	Important	Elevation of Privilege	4524153	Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4519998 Security Update	Important	Elevation of Privilege	4524152	Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4519998 Security Update	Important	Elevation of Privilege	4524152	Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4519998 Security Update	Important	Elevation of Privilege	4524152	Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4519998 Security Update	Important	Elevation of Privilege	4524152	Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1316						
Windows 10 Version 1703 for 32-bit Systems	4520010 Security Update	Important	Elevation of Privilege	4524151	Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4520010 Security Update	Important	Elevation of Privilege	4524151	Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4520004 Security Update	Important	Elevation of Privilege	4524150	Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4520004 Security Update	Important	Elevation of Privilege	4524150	Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4520008 Security Update	Important	Elevation of Privilege	4524149	Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1316						
Windows 10 Version 1803 for x64-based Systems	4520008 Security Update	Important	Elevation of Privilege	4524149	Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4520008 Security Update	Important	Elevation of Privilege	4524149	Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4520008 Security Update	Important	Elevation of Privilege	4524149	Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for	4519338 Security	Important	Elevation of Privilege	4524148	Base: 7.3 Temporal: 6.6	Yes

CVE-2019-1316						
x64-based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:H/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1809 for ARM64-based Systems	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2019	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4520004 Security Update	Important	Elevation of Privilege	4524150	Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1316						
Windows 10 Version 1903 for 32-bit Systems	4517389 Security Update	Important	Elevation of Privilege	4524147	Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4517389 Security Update	Important	Elevation of Privilege	4524147	Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4517389 Security Update	Important	Elevation of Privilege	4524147	Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4517389 Security Update	Important	Elevation of Privilege	4524147	Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1317 - Microsoft Windows Denial of Service Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1317 MITRE NVD	**CVE Title:** Microsoft Windows Denial of Service Vulnerability **Description:** A denial of service vulnerability exists when Windows improperly handles hard links. An attacker who successfully exploited the vulnerability could cause a target system to stop responding. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The vulnerability would allow an attacker to overwrite system files. The update addresses the vulnerability by correcting ACLs to system files. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/08/2019 07:00:00	Important	Denial of Service

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1317						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	4520011 Security Update	Important	Denial of Service	4524153	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:N/I:L/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4520011 Security Update	Important	Denial of Service	4524153	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:N/I:L/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1317						
Windows Server 2016	4519998 Security Update	Important	Denial of Service	4524152	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:N/I:L/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4519998 Security Update	Important	Denial of Service	4524152	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:N/I:L/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4519998 Security Update	Important	Denial of Service	4524152	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:N/I:L/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4519998 Security Update	Important	Denial of Service	4524152	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:N/I:L/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4520010 Security Update	Important	Denial of Service	4524151	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:N/I:L/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1317						
Windows 10 Version 1703 for x64-based Systems	4520010 Security Update	Important	Denial of Service	4524151	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:N/I:L/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4520004 Security Update	Important	Denial of Service	4524150	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:N/I:L/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4520004 Security Update	Important	Denial of Service	4524150	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:N/I:L/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4520008 Security Update	Important	Denial of Service	4524149	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:N/I:L/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4520008 Security Update	Important	Denial of Service	4524149	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:N/I:L/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1317						
Windows Server, version 1803 (Server Core Installation)	4520008 Security Update	Important	Denial of Service	4524149	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:N/I:L/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4520008 Security Update	Important	Denial of Service	4524149	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:N/I:L/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4519338 Security Update	Important	Denial of Service	4524148	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:N/I:L/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4519338 Security Update	Important	Denial of Service	4524148	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:N/I:L/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-	4519338 Security Update	Important	Denial of Service	4524148	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:N/I:L/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1317						
based Systems						
Windows Server 2019	4519338 Security Update	Important	Denial of Service	4524148	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:N/I:L/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4519338 Security Update	Important	Denial of Service	4524148	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:N/I:L/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4520004 Security Update	Important	Denial of Service	4524150	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:N/I:L/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4517389 Security Update	Important	Denial of Service	4524147	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:N/I:L/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-	4517389 Security Update	Important	Denial of Service	4524147	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:N/I:L/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1317						
based Systems						
Windows 10 Version 1903 for ARM64-based Systems	4517389 Security Update	Important	Denial of Service	4524147	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:N/I:L/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4517389 Security Update	Important	Denial of Service	4524147	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:N/I:L/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1318 - Microsoft Windows Transport Layer Security Spoofing Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-	**CVE Title:** Microsoft Windows Transport Layer Security Spoofing Vulnerability **Description:**	Important	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
1318 MITRE NVD	A spoofing vulnerability exists when Transport Layer Security (TLS) accesses non-Extended Master Secret (EMS) sessions. An attacker who successfully exploited this vulnerability may gain access to unauthorized information. To exploit the vulnerability, an attacker would have to conduct a man-in-the-middle attack. The update addresses the vulnerability by correcting how TLS client and server establish and resume sessions with non-EMS peers. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/08/2019 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1318						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4520003 Security Only 4519976 Monthly Rollup	Important	Spoofing	4524157	Base: 7.7 Temporal: 6.9 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4519976 Monthly Rollup 4520003 Security Only	Important	Spoofing	4524157	Base: 7.7 Temporal: 6.9 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2008	4519976 Monthly	Important	Spoofing	4524157	Base: 7.7 Temporal: 6.9	Yes

CVE-2019-1318						
R2 for x64-based Systems Service Pack 1 (Server Core installation)	Rollup 4520003 Security Only				Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L/E:P/RL:O/RC:C	
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4519976 Monthly Rollup 4520003 Security Only	Important	Spoofing	4524157	Base: 7.7 Temporal: 6.9 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4519976 Monthly Rollup 4520003 Security Only	Important	Spoofing	4524157	Base: 7.7 Temporal: 6.9 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L/E:P/RL:O/RC:C	Yes

CVE-2019-1318						
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4520002 Monthly Rollup 4520009 Security Only	Important	Spoofing	4516026	Base: 7.7 Temporal: 6.9 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2012	4519985 Security Only 4520007 Monthly Rollup	Important	Spoofing	4524154	Base: 7.7 Temporal: 6.9 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4519985 Security Only 4520007 Monthly Rollup	Important	Spoofing	4524154	Base: 7.7 Temporal: 6.9 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L/E:P/RL:O/RC:C	Yes

CVE-2019-1318						
Windows 8.1 for 32-bit systems	4519990 Security Only 4520005 Monthly Rollup	Important	Spoofing	4524156	Base: 7.7 Temporal: 6.9 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4519990 Security Only 4520005 Monthly Rollup	Important	Spoofing	4524156	Base: 7.7 Temporal: 6.9 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4519990 Security Only 4520005 Monthly Rollup	Important	Spoofing	4524156	Base: 7.7 Temporal: 6.9 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4520005 Monthly	Important	Spoofing	4524156	Base: 7.7 Temporal: 6.9	Yes

CVE-2019-1318						
	Rollup				Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L/E:P/RL:O/RC:C	
Windows Server 2012 R2 (Server Core installation)	4519990 Security Only 4520005 Monthly Rollup	Important	Spoofing	4524156	Base: 7.7 Temporal: 6.9 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4520011 Security Update	Important	Spoofing	4524153	Base: 7.7 Temporal: 6.9 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4520011 Security Update	Important	Spoofing	4524153	Base: 7.7 Temporal: 6.9 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2016	4519998 Security Update	Important	Spoofing	4524152	Base: 7.7 Temporal: 6.9 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version	4519998 Security	Important	Spoofing	4524152	Base: 7.7 Temporal: 6.9	Yes

CVE-2019-1318						
1607 for 32-bit Systems	Update				Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L/E:P/RL:O/RC:C	
Windows 10 Version 1607 for x64-based Systems	4519998 Security Update	Important	Spoofing	4524152	Base: 7.7 Temporal: 6.9 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4519998 Security Update	Important	Spoofing	4524152	Base: 7.7 Temporal: 6.9 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4520010 Security Update	Important	Spoofing	4524151	Base: 7.7 Temporal: 6.9 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4520010 Security Update	Important	Spoofing	4524151	Base: 7.7 Temporal: 6.9 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version	4520004 Security	Important	Spoofing	4524150	Base: 7.7 Temporal: 6.9	Yes

CVE-2019-1318						
1709 for 32-bit Systems	Update				Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L/E:P/RL:O/RC:C	
Windows 10 Version 1709 for x64-based Systems	4520004 Security Update	Important	Spoofing	4524150	Base: 7.7 Temporal: 6.9 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4520008 Security Update	Important	Spoofing	4524149	Base: 7.7 Temporal: 6.9 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4520008 Security Update	Important	Spoofing	4524149	Base: 7.7 Temporal: 6.9 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4520008 Security Update	Important	Spoofing	4524149	Base: 7.7 Temporal: 6.9 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version	4520008 Security	Important	Spoofing	4524149	Base: 7.7 Temporal: 6.9	Yes

CVE-2019-1318						
1803 for ARM64-based Systems	Update				Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L/E:P/RL:O/RC:C	
Windows 10 Version 1809 for 32-bit Systems	4519338 Security Update	Important	Spoofing	4524148	Base: 7.7 Temporal: 6.9 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4519338 Security Update	Important	Spoofing	4524148	Base: 7.7 Temporal: 6.9 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4519338 Security Update	Important	Spoofing	4524148	Base: 7.7 Temporal: 6.9 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2019	4519338 Security Update	Important	Spoofing	4524148	Base: 7.7 Temporal: 6.9 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L/E:P/RL:O/RC:C	Yes

CVE-2019-1318						
Windows Server 2019 (Server Core installation)	4519338 Security Update	Important	Spoofing	4524148	Base: 7.7 Temporal: 6.9 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4520004 Security Update	Important	Spoofing	4524150	Base: 7.7 Temporal: 6.9 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4517389 Security Update	Important	Spoofing	4524147	Base: 7.7 Temporal: 6.9 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4517389 Security Update	Important	Spoofing	4524147	Base: 7.7 Temporal: 6.9 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-	4517389 Security Update	Important	Spoofing	4524147	Base: 7.7 Temporal: 6.9 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L/E:P/RL:O/RC:C	Yes

CVE-2019-1318						
based Systems						
Windows Server, version 1903 (Server Core installation)	4517389 Security Update	Important	Spoofing	4524147	Base: 7.7 Temporal: 6.9 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4520002 Monthly Rollup 4520009 Security Only	Important	Spoofing	4516026	Base: 7.7 Temporal: 6.9 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4520002 Monthly Rollup 4520009 Security Only	Important	Spoofing	4516026	Base: 7.7 Temporal: 6.9 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2008	4520002 Monthly	Important	Spoofing	4516026	Base: 7.7 Temporal: 6.9	Yes

CVE-2019-1318						
for x64-based Systems Service Pack 2	Rollup 4520009 Security Only				Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L/E:P/RL:O/RC:C	
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4520002 Monthly Rollup 4520009 Security Only	Important	Spoofing	4516026	Base: 7.7 Temporal: 6.9 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L/E:P/RL:O/RC:C	Yes

CVE-2019-1319 - Windows Error Reporting Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1319 MITRE NVD	**CVE Title:** Windows Error Reporting Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files. The vulnerability could allow elevation of privilege if an attacker can successfully exploit it. An attacker who successfully exploited the vulnerability could gain greater access to sensitive information and system functionality. To exploit the vulnerability, an attacker could run a specially crafted application. The security update addresses the vulnerability by correcting the way that WER handles and executes files. **FAQ:** None **Mitigations:** None	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Workarounds: None **Revision:** 1.0 10/08/2019 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1319						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4520003 Security Only 4519976 Monthly	Important	Elevation of Privilege	4524157	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1319						
	Rollup					
Windows 7 for x64-based Systems Service Pack 1	4519976 Monthly Rollup 4520003 Security Only	Important	Elevation of Privilege	4524157	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4519976 Monthly Rollup 4520003 Security Only	Important	Elevation of Privilege	4524157	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based	4519976 Monthly Rollup 4520003 Security	Important	Elevation of Privilege	4524157	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1319						
Systems Service Pack 1	Only					
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4519976 Monthly Rollup 4520003 Security Only	Important	Elevation of Privilege	4524157	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4520002 Monthly Rollup 4520009 Security Only	Important	Elevation of Privilege	4516026	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012	4519985 Security Only 4520007 Monthly	Important	Elevation of Privilege	4524154	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1319						
	Rollup					
Windows Server 2012 (Server Core installation)	4519985 Security Only 4520007 Monthly Rollup	Important	Elevation of Privilege	4524154	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4519990 Security Only 4520005 Monthly Rollup	Important	Elevation of Privilege	4524156	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4519990 Security Only 4520005 Monthly Rollup	Important	Elevation of Privilege	4524156	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1319						
Windows Server 2012 R2	4519990 Security Only 4520005 Monthly Rollup	Important	Elevation of Privilege	4524156	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4520005 Monthly Rollup	Important	Elevation of Privilege	4524156	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4519990 Security Only 4520005 Monthly Rollup	Important	Elevation of Privilege	4524156	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4520011 Security Update	Important	Elevation of Privilege	4524153	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1319						
Windows 10 for x64-based Systems	4520011 Security Update	Important	Elevation of Privilege	4524153	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4519998 Security Update	Important	Elevation of Privilege	4524152	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4519998 Security Update	Important	Elevation of Privilege	4524152	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4519998 Security Update	Important	Elevation of Privilege	4524152	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4519998 Security Update	Important	Elevation of Privilege	4524152	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1319						
Windows 10 Version 1703 for 32-bit Systems	4520010 Security Update	Important	Elevation of Privilege	4524151	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4520010 Security Update	Important	Elevation of Privilege	4524151	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4520004 Security Update	Important	Elevation of Privilege	4524150	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4520004 Security Update	Important	Elevation of Privilege	4524150	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for	4520008 Security	Important	Elevation of Privilege	4524149	Base: 7 Temporal: 6.3	Yes

CVE-2019-1319						
32-bit Systems	Update				Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1803 for x64-based Systems	4520008 Security Update	Important	Elevation of Privilege	4524149	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4520008 Security Update	Important	Elevation of Privilege	4524149	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4520008 Security Update	Important	Elevation of Privilege	4524149	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1319						
32-bit Systems						
Windows 10 Version 1809 for x64-based Systems	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1319						
Windows 10 Version 1709 for ARM64-based Systems	4520004 Security Update	Important	Elevation of Privilege	4524150	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4517389 Security Update	Important	Elevation of Privilege	4524147	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4517389 Security Update	Important	Elevation of Privilege	4524147	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4517389 Security Update	Important	Elevation of Privilege	4524147	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1319						
Windows Server, version 1903 (Server Core installation)	4517389 Security Update	Important	Elevation of Privilege	4524147	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4520002 Monthly Rollup 4520009 Security Only	Important	Elevation of Privilege	4516026	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4520002 Monthly Rollup 4520009 Security Only	Important	Elevation of Privilege	4516026	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-	4520002 Monthly Rollup	Important	Elevation of Privilege	4516026	Base: 7 Temporal: 6.3	Yes

CVE-2019-1319						
based Systems Service Pack 2	4520009 Security Only				Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4520002 Monthly Rollup 4520009 Security Only	Important	Elevation of Privilege	4516026	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1320 - Microsoft Windows Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1320	**CVE Title:** Microsoft Windows Elevation of Privilege Vulnerability **Description:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	An elevation of privilege vulnerability exists when Windows improperly handles authentication requests. An attacker who successfully exploited this vulnerability could run processes in an elevated context. An attacker could exploit this vulnerability by running a specially crafted application on the victim system. The update addresses the vulnerability by correcting the way Windows handles authentication requests. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/08/2019 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1320						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1709 for 32-bit Systems	4520004 Security Update	Important	Elevation of Privilege	4524150	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4520004 Security Update	Important	Elevation of Privilege	4524150	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4520008 Security Update	Important	Elevation of Privilege	4524149	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for	4520008 Security	Important	Elevation of Privilege	4524149	Base: 7 Temporal: 6.3	Yes

CVE-2019-1320						
x64-based Systems	Update				Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:L/A:L/E:P/RL:O/RC:C	
Windows Server, version 1803 (Server Core Installation)	4520008 Security Update	Important	Elevation of Privilege	4524149	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4520008 Security Update	Important	Elevation of Privilege	4524149	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2019-1320						
Windows 10 Version 1809 for ARM64-based Systems	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2019	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4520004 Security Update	Important	Elevation of Privilege	4524150	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version	4517389 Security	Important	Elevation of Privilege	4524147	Base: 7 Temporal: 6.3	Yes

CVE-2019-1320						
1903 for 32-bit Systems	Update				Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:L/A:L/E:P/RL:O/RC:C	
Windows 10 Version 1903 for x64-based Systems	4517389 Security Update	Important	Elevation of Privilege	4524147	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4517389 Security Update	Important	Elevation of Privilege	4524147	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4517389 Security Update	Important	Elevation of Privilege	4524147	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2019-1321 - Microsoft Windows CloudStore Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1321 MITRE NVD	**CVE Title:** Microsoft Windows CloudStore Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when Windows CloudStore improperly handles file Discretionary Access Control List (DACL). An attacker who successfully exploited this vulnerability could overwrite a targeted file leading to an elevated status. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. The security update addresses the vulnerability by correcting how Windows CloudStore handles DACLs. **FAQ:** None **Mitigations:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Workarounds:** None **Revision:** 1.0 10/08/2019 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1321						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1703 for 32-bit Systems	4520010 Security Update	Important	Elevation of Privilege	4524151	Base: 5.8 Temporal: 5.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2019-1321						
Windows 10 Version 1703 for x64-based Systems	4520010 Security Update	Important	Elevation of Privilege	4524151	Base: 5.8 Temporal: 5.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4520004 Security Update	Important	Elevation of Privilege	4524150	Base: 5.8 Temporal: 5.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4520004 Security Update	Important	Elevation of Privilege	4524150	Base: 5.8 Temporal: 5.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4520008 Security Update	Important	Elevation of Privilege	4524149	Base: 5.8 Temporal: 5.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4520008 Security Update	Important	Elevation of Privilege	4524149	Base: 5.8 Temporal: 5.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2019-1321						
Windows Server, version 1803 (Server Core Installation)	4520008 Security Update	Important	Elevation of Privilege	4524149	Base: 5.8 Temporal: 5.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4520008 Security Update	Important	Elevation of Privilege	4524149	Base: 5.8 Temporal: 5.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 5.8 Temporal: 5.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 5.8 Temporal: 5.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2019-1321						
Windows 10 Version 1809 for ARM64-based Systems	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 5.8 Temporal: 5.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2019	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 5.8 Temporal: 5.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 5.8 Temporal: 5.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4520004 Security Update	Important	Elevation of Privilege	4524150	Base: 5.8 Temporal: 5.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version	4517389 Security	Important	Elevation of Privilege	4524147	Base: 5.8 Temporal: 5.2	Yes

CVE-2019-1321						
1903 for 32-bit Systems	Update				Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	
Windows 10 Version 1903 for x64-based Systems	4517389 Security Update	Important	Elevation of Privilege	4524147	Base: 5.8 Temporal: 5.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4517389 Security Update	Important	Elevation of Privilege	4524147	Base: 5.8 Temporal: 5.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4517389 Security Update	Important	Elevation of Privilege	4524147	Base: 5.8 Temporal: 5.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2019-1322 - Microsoft Windows Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1322 MITRE NVD	**CVE Title:** Microsoft Windows Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when Windows improperly handles authentication requests. An attacker who successfully exploited this vulnerability could run processes in an elevated context. An attacker could exploit this vulnerability by running a specially crafted application on the victim system. The update addresses the vulnerability by correcting the way Windows handles authentication requests. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/08/2019 07:00:00	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1322						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4520008 Security Update	Important	Elevation of Privilege	4524149	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4520008 Security Update	Important	Elevation of Privilege	4524149	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1322						
Windows Server, version 1803 (Server Core Installation)	4520008 Security Update	Important	Elevation of Privilege	4524149	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4520008 Security Update	Important	Elevation of Privilege	4524149	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1322						
Windows 10 Version 1809 for ARM64-based Systems	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4517389 Security Update	Important	Elevation of Privilege	4524147	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for	4517389 Security	Important	Elevation of Privilege	4524147	Base: 7 Temporal: 6.3	Yes

CVE-2019-1322						
x64-based Systems	Update				Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1903 for ARM64-based Systems	4517389 Security Update	Important	Elevation of Privilege	4524147	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4517389 Security Update	Important	Elevation of Privilege	4524147	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1323 - Microsoft Windows Update Client Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1323 MITRE NVD	**CVE Title:** Microsoft Windows Update Client Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in the Microsoft Windows Update Client when it does not properly handle privileges. An attacker who successfully exploited this vulnerability could run processes in an elevated context. An attacker could then install programs; view, change or delete data. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. The security update addresses the vulnerability by enabling the Windows Update client to properly handle user privileges. **FAQ:** None	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 10/08/2019 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1323						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version	4519338 Security	Important	Elevation of Privilege	4524148	Base: 7 Temporal: 6.3	Yes

CVE-2019-1323						
1809 for 32-bit Systems	Update				Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:L/I:H/A:L/E:P/RL:O/RC:C	
Windows 10 Version 1809 for x64-based Systems	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:L/I:H/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:L/I:H/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2019	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:L/I:H/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:L/I:H/A:L/E:P/RL:O/RC:C	Yes

CVE-2019-1323						
Windows 10 Version 1903 for 32-bit Systems	4517389 Security Update	Important	Elevation of Privilege	4524147	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:L/I:H/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4517389 Security Update	Important	Elevation of Privilege	4524147	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:L/I:H/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4517389 Security Update	Important	Elevation of Privilege	4524147	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:L/I:H/A:L/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4517389 Security Update	Important	Elevation of Privilege	4524147	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:L/I:H/A:L/E:P/RL:O/RC:C	Yes

CVE-2019-1325 - Windows Redirected Drive Buffering System Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1325 MITRE NVD	**CVE Title:** Windows Redirected Drive Buffering System Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in the Windows redirected drive buffering system (rdbss.sys) when the operating system improperly handles specific local calls within Windows 7 for 32-bit systems. When this vulnerability is exploited within other versions of Windows it can cause a denial of service, but not an elevation of privilege. To exploit this vulnerability, a low-level authenticated attacker could run a specially crafted application. The security update addresses the vulnerability by correcting how rdbss.sys handles these local calls. **FAQ:** None	Moderate	Denial of Service

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 10/08/2019 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1325						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems	4520003 Security Only	Important	Elevation of Privilege	4524157	Base: 7.8 Temporal: 7	Yes

CVE-2019-1325						
Service Pack 1	4519976 Monthly Rollup				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 7 for x64-based Systems Service Pack 1	4519976 Monthly Rollup 4520003 Security Only	Moderate	Denial of Service	4524157	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4519976 Monthly Rollup 4520003 Security Only	Moderate	Denial of Service	4524157	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for	4519976 Monthly Rollup	Moderate	Denial of Service	4524157	Base: 5.5 Temporal: 5	Yes

CVE-2019-1325						
Itanium-Based Systems Service Pack 1	4520003 Security Only				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4519976 Monthly Rollup 4520003 Security Only	Moderate	Denial of Service	4524157	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012	4519985 Security Only 4520007 Monthly Rollup	Moderate	Denial of Service	4524154	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4519985 Security Only 4520007	Moderate	Denial of Service	4524154	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1325						
	Monthly Rollup					
Windows 8.1 for 32-bit systems	4519990 Security Only 4520005 Monthly Rollup	Moderate	Denial of Service	4524156	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4519990 Security Only 4520005 Monthly Rollup	Moderate	Denial of Service	4524156	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4519990 Security Only 4520005 Monthly	Moderate	Denial of Service	4524156	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1325						
	Rollup					
Windows RT 8.1	4520005 Monthly Rollup	Moderate	Denial of Service	4524156	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4519990 Security Only 4520005 Monthly Rollup	Moderate	Denial of Service	4524156	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4520011 Security Update	Moderate	Denial of Service	4524153	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4520011 Security Update	Moderate	Denial of Service	4524153	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4519998 Security	Moderate	Denial of Service	4524152	Base: 5.5 Temporal: 5	Yes

CVE-2019-1325						
	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1607 for 32-bit Systems	4519998 Security Update	Moderate	Denial of Service	4524152	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4519998 Security Update	Moderate	Denial of Service	4524152	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4519998 Security Update	Moderate	Denial of Service	4524152	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4520010 Security Update	Moderate	Denial of Service	4524151	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for	4520010 Security Update	Moderate	Denial of Service	4524151	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1325						
x64-based Systems						
Windows 10 Version 1709 for 32-bit Systems	4520004 Security Update	Moderate	Denial of Service	4524150	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4520004 Security Update	Moderate	Denial of Service	4524150	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4520008 Security Update	Moderate	Denial of Service	4524149	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4520008 Security Update	Moderate	Denial of Service	4524149	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version	4520008 Security	Moderate	Denial of Service	4524149	Base: 5.5 Temporal: 5	Yes

CVE-2019-1325						
1803 (Server Core Installation)	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1803 for ARM64-based Systems	4520008 Security Update	Moderate	Denial of Service	4524149	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4519338 Security Update	Moderate	Denial of Service	4524148	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4519338 Security Update	Moderate	Denial of Service	4524148	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-	4519338 Security Update	Moderate	Denial of Service	4524148	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1325						
based Systems						
Windows Server 2019	4519338 Security Update	Moderate	Denial of Service	4524148	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4519338 Security Update	Moderate	Denial of Service	4524148	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4520004 Security Update	Moderate	Denial of Service	4524150	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4517389 Security Update	Moderate	Denial of Service	4524147	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for	4517389 Security	Moderate	Denial of Service	4524147	Base: 5.5 Temporal: 5	Yes

CVE-2019-1325						
x64-based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1903 for ARM64-based Systems	4517389 Security Update	Moderate	Denial of Service	4524147	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4517389 Security Update	Moderate	Denial of Service	4524147	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1326 - Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1326 MITRE NVD	**CVE Title:** Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability **Description:** A denial of service vulnerability exists in Remote Desktop Protocol (RDP) when an attacker connects to the target system using RDP and sends specially crafted requests. An attacker who successfully exploited this vulnerability could cause the RDP service on the target system to stop responding. To exploit this vulnerability, an attacker would need to run a specially crafted application against a server which provides Remote Desktop Protocol (RDP) services. The update addresses the vulnerability by correcting how RDP handles connection requests. **FAQ:** None **Mitigations:**	Important	Denial of Service

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Workarounds:** None **Revision:** 1.0 10/08/2019 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1326						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems	4520003 Security Only 4519976	Important	Denial of Service	4524157	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1326						
Service Pack 1	Monthly Rollup					
Windows 7 for x64-based Systems Service Pack 1	4519976 Monthly Rollup 4520003 Security Only	Important	Denial of Service	4524157	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4519976 Monthly Rollup 4520003 Security Only	Important	Denial of Service	4524157	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-	4519976 Monthly Rollup 4520003	Important	Denial of Service	4524157	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1326						
Based Systems Service Pack 1	Security Only					
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4519976 Monthly Rollup 4520003 Security Only	Important	Denial of Service	4524157	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4520002 Monthly Rollup 4520009 Security Only	Important	Denial of Service	4516026	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012	4519985 Security Only 4520007	Important	Denial of Service	4524154	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1326						
	Monthly Rollup					
Windows Server 2012 (Server Core installation)	4519985 Security Only 4520007 Monthly Rollup	Important	Denial of Service	4524154	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4519990 Security Only 4520005 Monthly Rollup	Important	Denial of Service	4524156	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4519990 Security Only 4520005 Monthly	Important	Denial of Service	4524156	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1326						
	Rollup					
Windows Server 2012 R2	4519990 Security Only 4520005 Monthly Rollup	Important	Denial of Service	4524156	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4520005 Monthly Rollup	Important	Denial of Service	4524156	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4519990 Security Only 4520005 Monthly Rollup	Important	Denial of Service	4524156	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4520011 Security	Important	Denial of Service	4524153	Base: 7.5 Temporal: 6.7	Yes

CVE-2019-1326						
	Update				Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	
Windows 10 for x64-based Systems	4520011 Security Update	Important	Denial of Service	4524153	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4519998 Security Update	Important	Denial of Service	4524152	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4519998 Security Update	Important	Denial of Service	4524152	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4519998 Security Update	Important	Denial of Service	4524152	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4519998 Security Update	Important	Denial of Service	4524152	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1326						
Windows 10 Version 1703 for 32-bit Systems	4520010 Security Update	Important	Denial of Service	4524151	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4520010 Security Update	Important	Denial of Service	4524151	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4520004 Security Update	Important	Denial of Service	4524150	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4520004 Security Update	Important	Denial of Service	4524150	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4520008 Security Update	Important	Denial of Service	4524149	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1326						
Windows 10 Version 1803 for x64-based Systems	4520008 Security Update	Important	Denial of Service	4524149	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4520008 Security Update	Important	Denial of Service	4524149	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4520008 Security Update	Important	Denial of Service	4524149	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4519338 Security Update	Important	Denial of Service	4524148	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for	4519338 Security	Important	Denial of Service	4524148	Base: 7.5 Temporal: 6.7	Yes

CVE-2019-1326						
x64-based Systems	Update				Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1809 for ARM64-based Systems	4519338 Security Update	Important	Denial of Service	4524148	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4519338 Security Update	Important	Denial of Service	4524148	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4519338 Security Update	Important	Denial of Service	4524148	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4520004 Security Update	Important	Denial of Service	4524150	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1326						
Windows 10 Version 1903 for 32-bit Systems	4517389 Security Update	Important	Denial of Service	4524147	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4517389 Security Update	Important	Denial of Service	4524147	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4517389 Security Update	Important	Denial of Service	4524147	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4517389 Security Update	Important	Denial of Service	4524147	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-	4520002 Monthly Rollup	Important	Denial of Service	4516026	Base: 7.5 Temporal: 6.7	Yes

CVE-2019-1326						
Based Systems Service Pack 2	4520009 Security Only				Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	
Windows Server 2008 for 32-bit Systems Service Pack 2	4520002 Monthly Rollup 4520009 Security Only	Important	Denial of Service	4516026	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4520002 Monthly Rollup 4520009 Security Only	Important	Denial of Service	4516026	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems	4520002 Monthly Rollup 4520009 Security	Important	Denial of Service	4516026	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1326						
Service Pack 2 (Server Core installation)	Only					

CVE-2019-1327 - Microsoft Excel Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1327 MITRE NVD	**CVE Title:** Microsoft Excel Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Excel. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) containing a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker would have to convince users to click a link, typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file. The security update addresses the vulnerability by correcting how Microsoft Excel handles objects in memory. **FAQ:** **Is the Preview Pane an attack vector for this vulnerability?** No, the Preview Pane is not an attack vector. **Mitigations:** None **Workarounds:**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 10/08/2019 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1327						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Excel 2010 Service Pack 2 (32-bit editions)	4484130 Security Update	Important	Remote Code Execution	4475574	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1327						
Microsoft Excel 2010 Service Pack 2 (64-bit editions)	4484130 Security Update	Important	Remote Code Execution	4475574	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2013 Service Pack 1 (32-bit editions)	4484123 Security Update	Important	Remote Code Execution	4475566	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2013 Service Pack 1 (64-bit editions)	4484123 Security Update	Important	Remote Code Execution	4475566	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2013 RT Service Pack 1	4484123 Security Update	Important	Remote Code Execution	4475566	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 for Mac	Release Notes Security Update	Important	Remote Code Execution	4475566	Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Excel 2016 (32-bit edition)	4484112 Security Update	Important	Remote Code Execution	4475579	Base: N/A Temporal:	Maybe

CVE-2019-1327						
					N/A Vector: N/A	
Microsoft Excel 2016 (64-bit edition)	4484112 Security Update	Important	Remote Code Execution	4475579	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2019 for 32-bit editions	Click to Run Security Update	Important	Remote Code Execution	4475579	Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Office 2019 for 64-bit editions	Click to Run Security Update	Important	Remote Code Execution	4475579	Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Office 2019 for Mac	Release Notes Security Update	Important	Remote Code Execution	4475579	Base: N/A Temporal: N/A Vector: N/A	No
Office 365 ProPlus for 32-bit Systems	Click to Run Security Update	Important	Remote Code Execution	4475579	Base: N/A Temporal: N/A Vector: N/A	No

CVE-2019-1327						
Office 365 ProPlus for 64-bit Systems	Click to Run Security Update	Important	Remote Code Execution	4475579	Base: N/A Temporal: N/A Vector: N/A	No

CVE-2019-1328 - Microsoft SharePoint Spoofing Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1328 MITRE NVD	**CVE Title:** Microsoft SharePoint Spoofing Vulnerability **Description:** A spoofing vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. These attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on	Important	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests. **FAQ:** **Is the Preview Pane an attack vector for this vulnerability?** No, the Preview Pane is not an attack vector. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/08/2019 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1328						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SharePoint Foundation 2010 Service Pack 2	4484131 Security Update	Important	Spoofing	4475605	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Foundation 2013 Service Pack 1	4484122 Security Update	Important	Spoofing	4484098	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Enterprise Server 2016	4484111 Security Update	Important	Spoofing	4475590	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1329 - Microsoft SharePoint Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1329 MITRE NVD	**CVE Title:** Microsoft SharePoint Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. These attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: **Is the Preview Pane an attack vector for this vulnerability?** No, the Preview Pane is not an attack vector. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/08/2019 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1329						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SharePoint Foundation 2010 Service Pack 2	4484131 Security Update	Important	Elevation of Privilege	4475605	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Foundation 2013 Service Pack 1	4484122 Security Update	Important	Elevation of Privilege	4484098	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Enterprise Server 2016	4484111 Security Update	Important	Elevation of Privilege	4475590	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1330 - Microsoft SharePoint Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1330 MITRE NVD	**CVE Title:** Microsoft SharePoint Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in Microsoft SharePoint. An attacker who successfully exploited this vulnerability could attempt to impersonate another user of the SharePoint server. To exploit this vulnerability, an authenticated attacker would send a specially crafted request to an affected server, thereby allowing the impersonation of another SharePoint user. The security update addresses the vulnerability by correcting how Microsoft SharePoint sanitizes user input. **FAQ:** **Is the Preview Pane an attack vector for this vulnerability?** No, the Preview Pane is not an attack vector.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 10/08/2019 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1330						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2019-1330						
Microsoft SharePoint Foundation 2013 Service Pack 1	4475608 Security Update	Important	Elevation of Privilege	4475557	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Enterprise Server 2016	4484111 Security Update	Important	Elevation of Privilege	4475590	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Server 2019	4484110 Security Update	Important	Elevation of Privilege	4475596	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1331 - Microsoft Excel Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1331	**CVE Title:** Microsoft Excel Remote Code Execution Vulnerability **Description:**	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Excel. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) containing a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker would have to convince users to click a link, typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file. The security update addresses the vulnerability by correcting how Microsoft Excel handles objects in memory.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: **Is the Preview Pane an attack vector for this vulnerability?** No, the Preview Pane is not an attack vector. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/08/2019 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1331						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Excel 2010 Service Pack 2 (32-bit editions)	4484130 Security Update	Important	Remote Code Execution	4475574	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2010 Service Pack 2 (64-bit editions)	4484130 Security Update	Important	Remote Code Execution	4475574	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (32-bit editions)	4475569 Security Update	Important	Remote Code Execution	4462224	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (64-bit editions)	4475569 Security Update	Important	Remote Code Execution	4462224	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2013 Service Pack 1 (32-bit editions)	4475558 Security Update	Important	Remote Code Execution	4464543	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1331						
Microsoft Office 2013 Service Pack 1 (64-bit editions)	4475558 Security Update	Important	Remote Code Execution	4464543	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2013 RT Service Pack 1	4475558 Security Update	Important	Remote Code Execution	4464543	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2013 Service Pack 1 (32-bit editions)	4484123 Security Update	Important	Remote Code Execution	4475566	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2013 Service Pack 1 (64-bit editions)	4484123 Security Update	Important	Remote Code Execution	4475566	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2013 RT Service Pack 1	4484123 Security Update	Important	Remote Code Execution	4475566	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 for Mac	Release Notes Security Update	Important	Remote Code Execution	4475566	Base: N/A Temporal:	No

CVE-2019-1331						
					N/A Vector: N/A	
Microsoft Excel 2016 (32-bit edition)	4484112 Security Update	Important	Remote Code Execution	4475579	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2016 (64-bit edition)	4484112 Security Update	Important	Remote Code Execution	4475579	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 (32-bit edition)	4475554 Security Update	Important	Remote Code Execution	4461539	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 (64-bit edition)	4475554 Security Update	Important	Remote Code Execution	4461539	Base: N/A Temporal: N/A Vector: N/A	Maybe
Office Online Server	4475595 Security Update	Important	Remote Code Execution	4475528	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1331						
Microsoft SharePoint Enterprise Server 2013 Service Pack 1	4462215 Security Update	Important	Remote Code Execution	4022236	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2019 for 32-bit editions	Click to Run Security Update	Important	Remote Code Execution	4022236	Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Office 2019 for 64-bit editions	Click to Run Security Update	Important	Remote Code Execution	4022236	Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Office 2019 for Mac	Release Notes Security Update	Important	Remote Code Execution	4022236	Base: N/A Temporal: N/A Vector: N/A	No
Office 365 ProPlus for 32-bit Systems	Click to Run Security Update	Important	Remote Code Execution	4022236	Base: N/A Temporal: N/A Vector: N/A	No
Office 365 ProPlus for 64-bit Systems	Click to Run Security Update	Important	Remote Code Execution	4022236	Base: N/A Temporal:	No

CVE-2019-1331						
					N/A Vector: N/A	
Excel Services on Microsoft SharePoint Server 2010 Service Pack 2	4462176 Security Update	Important	Remote Code Execution	4461569	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1333 - Remote Desktop Client Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1333 MITRE NVD	**CVE Title:** Remote Desktop Client Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server. An attacker who successfully exploited this vulnerability could execute arbitrary code on the computer of the connecting client. An	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would need to have control of a server and then convince a user to connect to it. An attacker would have no way of forcing a user to connect to the malicious server, they would need to trick the user into connecting via social engineering, DNS poisoning or using a Man in the Middle (MITM) technique. An attacker could also compromise a legitimate server, host malicious code on it, and wait for the user to connect. The update addresses the vulnerability by correcting how the Windows Remote Desktop Client handles connection requests. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/08/2019 07:00:00 Information published.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1333						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4520003 Security Only 4519976 Monthly Rollup	Critical	Remote Code Execution	4524157	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems	4519976 Monthly Rollup 4520003	Critical	Remote Code Execution	4524157	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1333						
Service Pack 1	Security Only					
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4519976 Monthly Rollup 4520003 Security Only	Critical	Remote Code Execution	4524157	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4519976 Monthly Rollup 4520003 Security Only	Critical	Remote Code Execution	4524157	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1333						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4519976 Monthly Rollup 4520003 Security Only	Critical	Remote Code Execution	4524157	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4520002 Monthly Rollup 4520009 Security Only	Critical	Remote Code Execution	4516026	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012	4519985 Security Only 4520007 Monthly Rollup	Critical	Remote Code Execution	4524154	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1333						
Windows Server 2012 (Server Core installation)	4519985 Security Only 4520007 Monthly Rollup	Critical	Remote Code Execution	4524154	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4519990 Security Only 4520005 Monthly Rollup	Critical	Remote Code Execution	4524156	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4519990 Security Only 4520005 Monthly Rollup	Critical	Remote Code Execution	4524156	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1333						
Windows Server 2012 R2	4519990 Security Only 4520005 Monthly Rollup	Critical	Remote Code Execution	4524156	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4520005 Monthly Rollup	Critical	Remote Code Execution	4524156	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4519990 Security Only 4520005 Monthly Rollup	Critical	Remote Code Execution	4524156	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4520011 Security Update	Critical	Remote Code Execution	4524153	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1333						
Windows 10 for x64-based Systems	4520011 Security Update	Critical	Remote Code Execution	4524153	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4519998 Security Update	Critical	Remote Code Execution	4524152	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4519998 Security Update	Critical	Remote Code Execution	4524152	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4519998 Security Update	Critical	Remote Code Execution	4524152	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4519998 Security Update	Critical	Remote Code Execution	4524152	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1333						
Windows 10 Version 1703 for 32-bit Systems	4520010 Security Update	Critical	Remote Code Execution	4524151	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4520010 Security Update	Critical	Remote Code Execution	4524151	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4520004 Security Update	Critical	Remote Code Execution	4524150	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4520004 Security Update	Critical	Remote Code Execution	4524150	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for	4520008 Security	Critical	Remote Code Execution	4524149	Base: 7.5 Temporal: 6.7	Yes

CVE-2019-1333						
32-bit Systems	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1803 for x64-based Systems	4520008 Security Update	Critical	Remote Code Execution	4524149	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4520008 Security Update	Critical	Remote Code Execution	4524149	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4520008 Security Update	Critical	Remote Code Execution	4524149	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for	4519338 Security	Critical	Remote Code Execution	4524148	Base: 7.5 Temporal: 6.7	Yes

CVE-2019-1333						
32-bit Systems	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1809 for x64-based Systems	4519338 Security Update	Critical	Remote Code Execution	4524148	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4519338 Security Update	Critical	Remote Code Execution	4524148	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4519338 Security Update	Critical	Remote Code Execution	4524148	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4519338 Security Update	Critical	Remote Code Execution	4524148	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1333						
Windows 10 Version 1709 for ARM64-based Systems	4520004 Security Update	Critical	Remote Code Execution	4524150	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4517389 Security Update	Critical	Remote Code Execution	4524147	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4517389 Security Update	Critical	Remote Code Execution	4524147	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4517389 Security Update	Critical	Remote Code Execution	4524147	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1333						
Windows Server, version 1903 (Server Core installation)	4517389 Security Update	Critical	Remote Code Execution	4524147	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4520002 Monthly Rollup 4520009 Security Only	Critical	Remote Code Execution	4516026	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4520002 Monthly Rollup 4520009 Security Only	Critical	Remote Code Execution	4516026	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1333						
Windows Server 2008 for x64-based Systems Service Pack 2	4520002 Monthly Rollup 4520009 Security Only	Critical	Remote Code Execution	4516026	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4520002 Monthly Rollup 4520009 Security Only	Critical	Remote Code Execution	4516026	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1334 - Windows Kernel Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1334 MITRE NVD	**CVE Title:** Windows Kernel Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory. An attacker who successfully exploited this vulnerability could obtain information to further compromise the userâ€™s system. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The vulnerability would not allow an attacker to execute code or to elevate user rights directly, but it could be used to obtain information that could be used to try to further compromise the affected system. The update addresses the vulnerability by correcting how the Windows kernel handles objects in memory. **FAQ:** **What type of information could be disclosed by this vulnerability?**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The type of information that could be disclosed if an attacker successfully exploited this vulnerability is the contents of Kernel memory. An attacker could read the contents of Kernel memory from a user mode process. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/08/2019 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1334						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 8.1 for 32-bit systems	4519990 Security Only 4520005 Monthly Rollup	Important	Information Disclosure	4524156	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4519990 Security Only 4520005 Monthly Rollup	Important	Information Disclosure	4524156	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1334						
Windows Server 2012 R2	4519990 Security Only 4520005 Monthly Rollup	Important	Information Disclosure	4524156	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4520005 Monthly Rollup	Important	Information Disclosure	4524156	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4519990 Security Only 4520005 Monthly Rollup	Important	Information Disclosure	4524156	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1334						
Windows 10 for 32-bit Systems	4520011 Security Update	Important	Information Disclosure	4524153	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4520011 Security Update	Important	Information Disclosure	4524153	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4519998 Security Update	Important	Information Disclosure	4524152	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4519998 Security Update	Important	Information Disclosure	4524152	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for	4519998 Security	Important	Information Disclosure	4524152	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2019-1334						
x64-based Systems	Update				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2016 (Server Core installation)	4519998 Security Update	Important	Information Disclosure	4524152	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4520010 Security Update	Important	Information Disclosure	4524151	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4520010 Security Update	Important	Information Disclosure	4524151	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4520004 Security Update	Important	Information Disclosure	4524150	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1334						
Windows 10 Version 1709 for x64-based Systems	4520004 Security Update	Important	Information Disclosure	4524150	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4520008 Security Update	Important	Information Disclosure	4524149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4520008 Security Update	Important	Information Disclosure	4524149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4520008 Security Update	Important	Information Disclosure	4524149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1334						
Windows 10 Version 1803 for ARM64-based Systems	4520008 Security Update	Important	Information Disclosure	4524149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4519338 Security Update	Important	Information Disclosure	4524148	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4519338 Security Update	Important	Information Disclosure	4524148	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4519338 Security Update	Important	Information Disclosure	4524148	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1334						
Windows Server 2019	4519338 Security Update	Important	Information Disclosure	4524148	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4519338 Security Update	Important	Information Disclosure	4524148	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4520004 Security Update	Important	Information Disclosure	4524150	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4517389 Security Update	Important	Information Disclosure	4524147	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1334						
Windows 10 Version 1903 for x64-based Systems	4517389 Security Update	Important	Information Disclosure	4524147	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4517389 Security Update	Important	Information Disclosure	4524147	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4517389 Security Update	Important	Information Disclosure	4524147	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1335 - Chakra Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1335 MITRE NVD	**CVE Title:** Chakra Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by modifying how the Chakra scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/08/2019 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1335						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge (EdgeHTML-based) on Windows 10 for 32-bit Systems	4520011 Security Update	Critical	Remote Code Execution	4524153	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 for x64-based Systems	4520011 Security Update	Critical	Remote Code Execution	4524153	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows Server 2016	4519998 Security Update	Moderate	Remote Code Execution	4524152	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1335						
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1607 for 32-bit Systems	4519998 Security Update	Critical	Remote Code Execution	4524152	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1607 for x64-based Systems	4519998 Security Update	Critical	Remote Code Execution	4524152	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version	4520010 Security Update	Critical	Remote Code Execution	4524151	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1335						
1703 for 32-bit Systems						
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1703 for x64-based Systems	4520010 Security Update	Critical	Remote Code Execution	4524151	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1709 for 32-bit Systems	4520004 Security Update	Critical	Remote Code Execution	4524150	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on	4520004 Security Update	Critical	Remote Code Execution	4524150	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1335						
Windows 10 Version 1709 for x64-based Systems						
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for 32-bit Systems	4520008 Security Update	Critical	Remote Code Execution	4524149	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for x64-based Systems	4520008 Security Update	Critical	Remote Code Execution	4524149	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1335						
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for ARM64-based Systems	4520008 Security Update	Critical	Remote Code Execution	4524149	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for 32-bit Systems	4519338 Security Update	Critical	Remote Code Execution	4524148	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10	4519338 Security Update	Critical	Remote Code Execution	4524148	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1335						
Version 1809 for x64-based Systems						
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for ARM64-based Systems	4519338 Security Update	Critical	Remote Code Execution	4524148	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows Server 2019	4519338 Security Update	Moderate	Remote Code Execution	4524148	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-	4520004 Security	Critical	Remote Code Execution	4524150	Base: 4.2 Temporal: 3.8	Yes

CVE-2019-1335						
based) on Windows 10 Version 1709 for ARM64-based Systems	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for 32-bit Systems	4517389 Security Update	Critical	Remote Code Execution	4524147	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for	4517389 Security Update	Critical	Remote Code Execution	4524147	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1335						
x64-based Systems						
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for ARM64-based Systems	4517389 Security Update	Critical	Remote Code Execution	4524147	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
ChakraCore	Release Notes Security Update	Critical	Remote Code Execution	4524147	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Maybe

CVE-2019-1336 - Microsoft Windows Update Client Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1336 MITRE NVD	**CVE Title:** Microsoft Windows Update Client Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in the Microsoft Windows Update Client when it does not properly handle privileges. An attacker who successfully exploited this vulnerability could run processes in an elevated context. An attacker could then install programs; view, change or delete data. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. The security update addresses the vulnerability by enabling the Windows Update client to properly handle user privileges. **FAQ:** None	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 10/08/2019 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1336						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version	4519338 Security	Important	Elevation of Privilege	4524148	Base: 7 Temporal: 6.3	Yes

CVE-2019-1336						
1809 for 32-bit Systems	Update				Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:L/I:H/A:L/E:P/RL:O/RC:C	
Windows 10 Version 1809 for x64-based Systems	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:L/I:H/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:L/I:H/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2019	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:L/I:H/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:L/I:H/A:L/E:P/RL:O/RC:C	Yes

CVE-2019-1336						
Windows 10 Version 1903 for 32-bit Systems	4517389 Security Update	Important	Elevation of Privilege	4524147	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:L/I:H/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4517389 Security Update	Important	Elevation of Privilege	4524147	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:L/I:H/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4517389 Security Update	Important	Elevation of Privilege	4524147	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:L/I:H/A:L/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4517389 Security Update	Important	Elevation of Privilege	4524147	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:L/I:H/A:L/E:P/RL:O/RC:C	Yes

CVE-2019-1337 - Windows Update Client Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1337 MITRE NVD	**CVE Title:** Windows Update Client Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when Windows Update Client fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could potentially disclose memory contents of an elevated process. To exploit this vulnerability, an authenticated attacker could run a specially crafted application in user mode. The update addresses the vulnerability by correcting how the Windows Update Client handles objects in memory. **FAQ:** **What type of information could be disclosed by this vulnerability?**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The type of information that could be disclosed if an attacker successfully exploited this vulnerability is the contents of Kernel memory. An attacker could read the contents of Kernel memory from a user mode process. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/08/2019 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1337						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1809 for 32-bit Systems	4519338 Security Update	Important	Information Disclosure	4524148	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4519338 Security Update	Important	Information Disclosure	4524148	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4519338 Security Update	Important	Information Disclosure	4524148	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2019	4519338 Security Update	Important	Information Disclosure	4524148	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1337						
Windows Server 2019 (Server Core installation)	4519338 Security Update	Important	Information Disclosure	4524148	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4517389 Security Update	Important	Information Disclosure	4524147	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4517389 Security Update	Important	Information Disclosure	4524147	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4517389 Security Update	Important	Information Disclosure	4524147	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1337						
Windows Server, version 1903 (Server Core installation)	4517389 Security Update	Important	Information Disclosure	4524147	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1338 - Windows NTLM Security Feature Bypass Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1338 MITRE NVD	**CVE Title:** Windows NTLM Security Feature Bypass Vulnerability **Description:** A security feature bypass vulnerability exists in Microsoft Windows when a man-in-the-middle attacker is able to successfully bypass the NTLMv2 protection if a client is also sending LMv2 responses. An attacker who successfully exploited this vulnerability could gain the ability to downgrade NTLM security features. To exploit this vulnerability, the attacker would need to be able to modify NTLM traffic exchange.	Important	Security Feature Bypass

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The update addresses the vulnerability by hardening NTLMv2 protection on the server-side. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/08/2019 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1338						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4520003 Security Only 4519976 Monthly Rollup	Important	Security Feature Bypass	4524157	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4519976 Monthly Rollup 4520003 Security Only	Important	Security Feature Bypass	4524157	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4519976 Monthly Rollup 4520003 Security Only	Important	Security Feature Bypass	4524157	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1338						
(Server Core installation)						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4519976 Monthly Rollup 4520003 Security Only	Important	Security Feature Bypass	4524157	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4519976 Monthly Rollup 4520003 Security Only	Important	Security Feature Bypass	4524157	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4520002 Monthly Rollup 4520009 Security	Important	Security Feature Bypass	4516026	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1338						
(Server Core installation)	Only					
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4520002 Monthly Rollup 4520009 Security Only	Important	Security Feature Bypass	4516026	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4520002 Monthly Rollup 4520009 Security Only	Important	Security Feature Bypass	4516026	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4520002 Monthly Rollup 4520009 Security Only	Important	Security Feature Bypass	4516026	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1338						
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4520002 Monthly Rollup 4520009 Security Only	Important	Security Feature Bypass	4516026	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1339 - Windows Error Reporting Manager Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1339 MITRE NVD	**CVE Title:** Windows Error Reporting Manager Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when Windows Error Reporting manager improperly handles hard links. An attacker who successfully exploited this vulnerability could overwrite a targeted file leading to an elevated status.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. The security update addresses the vulnerability by correcting how Windows Error Reporting manager handles hard links. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/08/2019 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1339						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4520003 Security Only 4519976 Monthly Rollup	Important	Elevation of Privilege	4524157	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4519976 Monthly Rollup 4520003 Security Only	Important	Elevation of Privilege	4524157	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server	4519976 Monthly Rollup 4520003 Security Only	Important	Elevation of Privilege	4524157	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1339						
Core installation)						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4519976 Monthly Rollup 4520003 Security Only	Important	Elevation of Privilege	4524157	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4519976 Monthly Rollup 4520003 Security Only	Important	Elevation of Privilege	4524157	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server	4520002 Monthly Rollup 4520009 Security	Important	Elevation of Privilege	4516026	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1339						
Core installation)	Only					
Windows Server 2012	4519985 Security Only 4520007 Monthly Rollup	Important	Elevation of Privilege	4524154	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4519985 Security Only 4520007 Monthly Rollup	Important	Elevation of Privilege	4524154	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4519990 Security Only 4520005 Monthly Rollup	Important	Elevation of Privilege	4524156	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1339						
Windows 8.1 for x64-based systems	4519990 Security Only 4520005 Monthly Rollup	Important	Elevation of Privilege	4524156	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4519990 Security Only 4520005 Monthly Rollup	Important	Elevation of Privilege	4524156	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4520005 Monthly Rollup	Important	Elevation of Privilege	4524156	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4519990 Security Only 4520005 Monthly	Important	Elevation of Privilege	4524156	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1339						
	Rollup					
Windows 10 for 32-bit Systems	4520011 Security Update	Important	Elevation of Privilege	4524153	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4520011 Security Update	Important	Elevation of Privilege	4524153	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4519998 Security Update	Important	Elevation of Privilege	4524152	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4519998 Security Update	Important	Elevation of Privilege	4524152	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4519998 Security Update	Important	Elevation of Privilege	4524152	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1339						
Windows Server 2016 (Server Core installation)	4519998 Security Update	Important	Elevation of Privilege	4524152	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4520010 Security Update	Important	Elevation of Privilege	4524151	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4520010 Security Update	Important	Elevation of Privilege	4524151	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4520004 Security Update	Important	Elevation of Privilege	4524150	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4520004 Security Update	Important	Elevation of Privilege	4524150	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1339						
Windows 10 Version 1803 for 32-bit Systems	4520008 Security Update	Important	Elevation of Privilege	4524149	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4520008 Security Update	Important	Elevation of Privilege	4524149	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4520008 Security Update	Important	Elevation of Privilege	4524149	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4520008 Security Update	Important	Elevation of Privilege	4524149	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1339						
Windows 10 Version 1809 for 32-bit Systems	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1339						
Windows 10 Version 1709 for ARM64-based Systems	4520004 Security Update	Important	Elevation of Privilege	4524150	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4517389 Security Update	Important	Elevation of Privilege	4524147	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4517389 Security Update	Important	Elevation of Privilege	4524147	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4517389 Security Update	Important	Elevation of Privilege	4524147	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1339						
Windows Server, version 1903 (Server Core installation)	4517389 Security Update	Important	Elevation of Privilege	4524147	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4520002 Monthly Rollup 4520009 Security Only	Important	Elevation of Privilege	4516026	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4520002 Monthly Rollup 4520009 Security Only	Important	Elevation of Privilege	4516026	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-	4520002 Monthly Rollup	Important	Elevation of Privilege	4516026	Base: 7.8 Temporal: 7	Yes

CVE-2019-1339						
based Systems Service Pack 2	4520009 Security Only				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4520002 Monthly Rollup 4520009 Security Only	Important	Elevation of Privilege	4516026	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1340 - Microsoft Windows Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1340	**CVE Title:** Microsoft Windows Elevation of Privilege Vulnerability **Description:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	An elevation of privilege vulnerability exists in Windows AppX Deployment Server that allows file creation in arbitrary locations. To exploit the vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. The update addresses the vulnerability by not permitting Windows AppX Deployment Server to create files in arbitrary locations. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/08/2019 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1340						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1703 for 32-bit Systems	4520010 Security Update	Important	Elevation of Privilege	4524151	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4520010 Security Update	Important	Elevation of Privilege	4524151	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4520004 Security Update	Important	Elevation of Privilege	4524150	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for	4520004 Security	Important	Elevation of Privilege	4524150	Base: 7.8 Temporal: 7	Yes

CVE-2019-1340						
x64-based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1803 for 32-bit Systems	4520008 Security Update	Important	Elevation of Privilege	4524149	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4520008 Security Update	Important	Elevation of Privilege	4524149	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4520008 Security Update	Important	Elevation of Privilege	4524149	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4520008 Security Update	Important	Elevation of Privilege	4524149	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1340						
Windows 10 Version 1809 for 32-bit Systems	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1340						
Windows 10 Version 1709 for ARM64-based Systems	4520004 Security Update	Important	Elevation of Privilege	4524150	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4517389 Security Update	Important	Elevation of Privilege	4524147	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4517389 Security Update	Important	Elevation of Privilege	4524147	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4517389 Security Update	Important	Elevation of Privilege	4524147	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1340						
Windows Server, version 1903 (Server Core installation)	4517389 Security Update	Important	Elevation of Privilege	4524147	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1341 - Windows Power Service Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1341 MITRE NVD	**CVE Title:** Windows Power Service Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when umpo.dll of the Power Service, improperly handles a Registry Restore Key function. An attacker who successfully exploited this vulnerability could delete a targeted registry key leading to an elevated status.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. The security update addresses the vulnerability by correcting how umpo.dll of the Power Service handles Registry Restore Key requests. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/08/2019 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1341						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4520003 Security Only 4519976 Monthly Rollup	Important	Elevation of Privilege	4524157	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4519976 Monthly Rollup 4520003 Security Only	Important	Elevation of Privilege	4524157	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1341						
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4519976 Monthly Rollup 4520003 Security Only	Important	Elevation of Privilege	4524157	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4519976 Monthly Rollup 4520003 Security Only	Important	Elevation of Privilege	4524157	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems	4519976 Monthly Rollup 4520003 Security	Important	Elevation of Privilege	4524157	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1341						
Service Pack 1	Only					
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4520002 Monthly Rollup 4520009 Security Only	Important	Elevation of Privilege	4516026	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012	4519985 Security Only 4520007 Monthly Rollup	Important	Elevation of Privilege	4524154	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4519985 Security Only 4520007 Monthly	Important	Elevation of Privilege	4524154	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1341						
	Rollup					
Windows 8.1 for 32-bit systems	4519990 Security Only 4520005 Monthly Rollup	Important	Elevation of Privilege	4524156	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4519990 Security Only 4520005 Monthly Rollup	Important	Elevation of Privilege	4524156	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4519990 Security Only 4520005 Monthly Rollup	Important	Elevation of Privilege	4524156	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1341						
Windows RT 8.1	4520005 Monthly Rollup	Important	Elevation of Privilege	4524156	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4519990 Security Only 4520005 Monthly Rollup	Important	Elevation of Privilege	4524156	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4520011 Security Update	Important	Elevation of Privilege	4524153	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4520011 Security Update	Important	Elevation of Privilege	4524153	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4519998 Security Update	Important	Elevation of Privilege	4524152	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1341						
Windows 10 Version 1607 for 32-bit Systems	4519998 Security Update	Important	Elevation of Privilege	4524152	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4519998 Security Update	Important	Elevation of Privilege	4524152	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4519998 Security Update	Important	Elevation of Privilege	4524152	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4520010 Security Update	Important	Elevation of Privilege	4524151	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4520010 Security Update	Important	Elevation of Privilege	4524151	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1341						
Windows 10 Version 1709 for 32-bit Systems	4520004 Security Update	Important	Elevation of Privilege	4524150	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4520004 Security Update	Important	Elevation of Privilege	4524150	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4520008 Security Update	Important	Elevation of Privilege	4524149	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4520008 Security Update	Important	Elevation of Privilege	4524149	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server	4520008 Security Update	Important	Elevation of Privilege	4524149	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1341						
Core Installation)						
Windows 10 Version 1803 for ARM64-based Systems	4520008 Security Update	Important	Elevation of Privilege	4524149	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1341						
Windows Server 2019	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4520004 Security Update	Important	Elevation of Privilege	4524150	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4517389 Security Update	Important	Elevation of Privilege	4524147	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4517389 Security Update	Important	Elevation of Privilege	4524147	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1341						
Windows 10 Version 1903 for ARM64-based Systems	4517389 Security Update	Important	Elevation of Privilege	4524147	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4517389 Security Update	Important	Elevation of Privilege	4524147	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4520002 Monthly Rollup 4520009 Security Only	Important	Elevation of Privilege	4516026	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems	4520002 Monthly Rollup 4520009	Important	Elevation of Privilege	4516026	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1341						
Service Pack 2	Security Only					
Windows Server 2008 for x64-based Systems Service Pack 2	4520002 Monthly Rollup 4520009 Security Only	Important	Elevation of Privilege	4516026	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4520002 Monthly Rollup 4520009 Security Only	Important	Elevation of Privilege	4516026	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1342 - Windows Error Reporting Manager Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1342 MITRE NVD	**CVE Title:** Windows Error Reporting Manager Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when Windows Error Reporting manager improperly handles a process crash. An attacker who successfully exploited this vulnerability could delete a targeted file leading to an elevated status. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. The security update addresses the vulnerability by correcting how Windows Error Reporting manager handles process crashes. **FAQ:** None **Mitigations:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Workarounds:** None **Revision:** 1.0 10/08/2019 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1342						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems	4520003 Security Only 4519976	Important	Elevation of Privilege	4524157	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1342						
Service Pack 1	Monthly Rollup					
Windows 7 for x64-based Systems Service Pack 1	4519976 Monthly Rollup 4520003 Security Only	Important	Elevation of Privilege	4524157	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4519976 Monthly Rollup 4520003 Security Only	Important	Elevation of Privilege	4524157	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-	4519976 Monthly Rollup 4520003	Important	Elevation of Privilege	4524157	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1342						
Based Systems Service Pack 1	Security Only					
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4519976 Monthly Rollup 4520003 Security Only	Important	Elevation of Privilege	4524157	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4520002 Monthly Rollup 4520009 Security Only	Important	Elevation of Privilege	4516026	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012	4519985 Security Only 4520007	Important	Elevation of Privilege	4524154	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1342						
	Monthly Rollup					
Windows Server 2012 (Server Core installation)	4519985 Security Only 4520007 Monthly Rollup	Important	Elevation of Privilege	4524154	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4519990 Security Only 4520005 Monthly Rollup	Important	Elevation of Privilege	4524156	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4519990 Security Only 4520005 Monthly	Important	Elevation of Privilege	4524156	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1342						
	Rollup					
Windows Server 2012 R2	4519990 Security Only 4520005 Monthly Rollup	Important	Elevation of Privilege	4524156	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4520005 Monthly Rollup	Important	Elevation of Privilege	4524156	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4519990 Security Only 4520005 Monthly Rollup	Important	Elevation of Privilege	4524156	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4520011 Security	Important	Elevation of Privilege	4524153	Base: 7 Temporal: 6.3	Yes

CVE-2019-1342						
	Update				Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 for x64-based Systems	4520011 Security Update	Important	Elevation of Privilege	4524153	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4519998 Security Update	Important	Elevation of Privilege	4524152	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4519998 Security Update	Important	Elevation of Privilege	4524152	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4519998 Security Update	Important	Elevation of Privilege	4524152	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4519998 Security	Important	Elevation of Privilege	4524152	Base: 7 Temporal: 6.3	Yes

CVE-2019-1342						
(Server Core installation)	Update				Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1703 for 32-bit Systems	4520010 Security Update	Important	Elevation of Privilege	4524151	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4520010 Security Update	Important	Elevation of Privilege	4524151	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4520004 Security Update	Important	Elevation of Privilege	4524150	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4520004 Security Update	Important	Elevation of Privilege	4524150	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1342						
Windows 10 Version 1803 for 32-bit Systems	4520008 Security Update	Important	Elevation of Privilege	4524149	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4520008 Security Update	Important	Elevation of Privilege	4524149	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4520008 Security Update	Important	Elevation of Privilege	4524149	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4520008 Security Update	Important	Elevation of Privilege	4524149	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1342						
Windows 10 Version 1809 for 32-bit Systems	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4519338 Security	Important	Elevation of Privilege	4524148	Base: 7 Temporal: 6.3	Yes

CVE-2019-1342						
(Server Core installation)	Update				Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1709 for ARM64-based Systems	4520004 Security Update	Important	Elevation of Privilege	4524150	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4517389 Security Update	Important	Elevation of Privilege	4524147	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4517389 Security Update	Important	Elevation of Privilege	4524147	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-	4517389 Security Update	Important	Elevation of Privilege	4524147	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1342						
based Systems						
Windows Server, version 1903 (Server Core installation)	4517389 Security Update	Important	Elevation of Privilege	4524147	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4520002 Monthly Rollup 4520009 Security Only	Important	Elevation of Privilege	4516026	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4520002 Monthly Rollup 4520009 Security Only	Important	Elevation of Privilege	4516026	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1342						
Windows Server 2008 for x64-based Systems Service Pack 2	4520002 Monthly Rollup 4520009 Security Only	Important	Elevation of Privilege	4516026	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4520002 Monthly Rollup 4520009 Security Only	Important	Elevation of Privilege	4516026	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1343 - Windows Denial of Service Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1343 MITRE NVD	**CVE Title:** Windows Denial of Service Vulnerability **Description:** A denial of service vulnerability exists when Windows improperly handles objects in memory. An attacker who successfully exploited the vulnerability could cause a target system to stop responding. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application or to convince a user to open a specific file on a network share. The vulnerability would not allow an attacker to execute code or to elevate user rights directly, but it could be used to cause a target system to stop responding. The update addresses the vulnerability by correcting how Windows handles objects in memory. **FAQ:** None **Mitigations:** None	Important	Denial of Service

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Workarounds: None **Revision:** 1.0 10/08/2019 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1343						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows Server 2012	4519985 Security Only 4520007 Monthly	Important	Denial of Service	4524154	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1343						
	Rollup					
Windows Server 2012 (Server Core installation)	4519985 Security Only 4520007 Monthly Rollup	Important	Denial of Service	4524154	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4519990 Security Only 4520005 Monthly Rollup	Important	Denial of Service	4524156	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4519990 Security Only 4520005 Monthly Rollup	Important	Denial of Service	4524156	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1343						
Windows Server 2012 R2	4519990 Security Only 4520005 Monthly Rollup	Important	Denial of Service	4524156	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4520005 Monthly Rollup	Important	Denial of Service	4524156	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4519990 Security Only 4520005 Monthly Rollup	Important	Denial of Service	4524156	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4520011 Security Update	Important	Denial of Service	4524153	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1343						
Windows 10 for x64-based Systems	4520011 Security Update	Important	Denial of Service	4524153	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4519998 Security Update	Important	Denial of Service	4524152	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4519998 Security Update	Important	Denial of Service	4524152	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4519998 Security Update	Important	Denial of Service	4524152	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4519998 Security Update	Important	Denial of Service	4524152	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1343						
Windows 10 Version 1703 for 32-bit Systems	4520010 Security Update	Important	Denial of Service	4524151	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4520010 Security Update	Important	Denial of Service	4524151	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4520004 Security Update	Important	Denial of Service	4524150	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4520004 Security Update	Important	Denial of Service	4524150	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4520008 Security Update	Important	Denial of Service	4524149	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1343						
Windows 10 Version 1803 for x64-based Systems	4520008 Security Update	Important	Denial of Service	4524149	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4520008 Security Update	Important	Denial of Service	4524149	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4520008 Security Update	Important	Denial of Service	4524149	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4519338 Security Update	Important	Denial of Service	4524148	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for	4519338 Security	Important	Denial of Service	4524148	Base: 6.5 Temporal: 5.9	Yes

CVE-2019-1343						
x64-based Systems	Update				Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1809 for ARM64-based Systems	4519338 Security Update	Important	Denial of Service	4524148	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4519338 Security Update	Important	Denial of Service	4524148	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4519338 Security Update	Important	Denial of Service	4524148	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4520004 Security Update	Important	Denial of Service	4524150	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1343						
Windows 10 Version 1903 for 32-bit Systems	4517389 Security Update	Important	Denial of Service	4524147	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4517389 Security Update	Important	Denial of Service	4524147	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4517389 Security Update	Important	Denial of Service	4524147	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4517389 Security Update	Important	Denial of Service	4524147	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1344 - Windows Code Integrity Module Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1344 MITRE NVD	**CVE Title:** Windows Code Integrity Module Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists in the way that the Windows Code Integrity Module handles objects in memory. An attacker who successfully exploited this vulnerability could obtain information to further compromise the userâ€™s system. To exploit the vulnerability, an attacker would have to log on to an affected system and run a specially crafted application or convince a target to run a crafted application. The security update addresses the vulnerability by modifying how the Code Integrity Module handles objects in memory. **FAQ:** **What type of information could be disclosed by this vulnerability?**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The type of information that could be disclosed if an attacker successfully exploited this vulnerability is the contents of Kernel memory. An attacker could read the contents of Kernel memory from a user mode process. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/08/2019 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1344						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4520003 Security Only 4519976 Monthly Rollup	Important	Information Disclosure	4524157	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4519976 Monthly Rollup 4520003 Security Only	Important	Information Disclosure	4524157	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4519976 Monthly Rollup 4520003 Security Only	Important	Information Disclosure	4524157	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1344						
(Server Core installation)						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4519976 Monthly Rollup 4520003 Security Only	Important	Information Disclosure	4524157	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4519976 Monthly Rollup 4520003 Security Only	Important	Information Disclosure	4524157	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems	4520002 Monthly Rollup 4520009 Security	Important	Information Disclosure	4516026	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1344						
Service Pack 2 (Server Core installation)	Only					
Windows Server 2012	4519985 Security Only 4520007 Monthly Rollup	Important	Information Disclosure	4524154	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4519985 Security Only 4520007 Monthly Rollup	Important	Information Disclosure	4524154	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4519990 Security Only 4520005	Important	Information Disclosure	4524156	Base: 5.5 Temporal: 5 Vector:	Yes

CVE-2019-1344						
	Monthly Rollup				CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 8.1 for x64-based systems	4519990 Security Only 4520005 Monthly Rollup	Important	Information Disclosure	4524156	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4519990 Security Only 4520005 Monthly Rollup	Important	Information Disclosure	4524156	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4520005 Monthly Rollup	Important	Information Disclosure	4524156	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1344						
Windows Server 2012 R2 (Server Core installation)	4519990 Security Only 4520005 Monthly Rollup	Important	Information Disclosure	4524156	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4520011 Security Update	Important	Information Disclosure	4524153	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4520011 Security Update	Important	Information Disclosure	4524153	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4519998 Security Update	Important	Information Disclosure	4524152	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1344						
Windows 10 Version 1607 for 32-bit Systems	4519998 Security Update	Important	Information Disclosure	4524152	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4519998 Security Update	Important	Information Disclosure	4524152	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4519998 Security Update	Important	Information Disclosure	4524152	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4520010 Security Update	Important	Information Disclosure	4524151	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version	4520010 Security	Important	Information Disclosure	4524151	Base: 5.5 Temporal: 5	Yes

CVE-2019-1344						
1703 for x64-based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1709 for 32-bit Systems	4520004 Security Update	Important	Information Disclosure	4524150	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4520004 Security Update	Important	Information Disclosure	4524150	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4520008 Security Update	Important	Information Disclosure	4524149	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4520008 Security Update	Important	Information Disclosure	4524149	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1344						
Windows Server, version 1803 (Server Core Installation)	4520008 Security Update	Important	Information Disclosure	4524149	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4520008 Security Update	Important	Information Disclosure	4524149	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4519338 Security Update	Important	Information Disclosure	4524148	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for	4519338 Security Update	Important	Information Disclosure	4524148	Base: 5.5 Temporal: 5 Vector:	Yes

CVE-2019-1344						
x64-based Systems					CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1809 for ARM64-based Systems	4519338 Security Update	Important	Information Disclosure	4524148	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2019	4519338 Security Update	Important	Information Disclosure	4524148	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4519338 Security Update	Important	Information Disclosure	4524148	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-	4520004 Security Update	Important	Information Disclosure	4524150	Base: 5.5 Temporal: 5 Vector:	Yes

CVE-2019-1344						
based Systems					CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1903 for 32-bit Systems	4517389 Security Update	Important	Information Disclosure	4524147	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4517389 Security Update	Important	Information Disclosure	4524147	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4517389 Security Update	Important	Information Disclosure	4524147	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server	4517389 Security Update	Important	Information Disclosure	4524147	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1344						
Core installation)						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4520002 Monthly Rollup 4520009 Security Only	Important	Information Disclosure	4516026	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4520002 Monthly Rollup 4520009 Security Only	Important	Information Disclosure	4516026	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems	4520002 Monthly Rollup 4520009 Security	Important	Information Disclosure	4516026	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1344						
Service Pack 2	Only					
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4520002 Monthly Rollup 4520009 Security Only	Important	Information Disclosure	4516026	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1345 - Windows Kernel Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1345	**CVE Title:** Windows Kernel Information Disclosure Vulnerability **Description:**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory. An attacker who successfully exploited this vulnerability could obtain information to further compromise the userâ€™s system. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The vulnerability would not allow an attacker to execute code or to elevate user rights directly, but it could be used to obtain information that could be used to try to further compromise the affected system. The update addresses the vulnerability by correcting how the Windows kernel handles objects in memory. **FAQ:** **What type of information could be disclosed by this vulnerability?** The type of information that could be disclosed if an attacker successfully exploited this vulnerability is the contents of Kernel memory. An attacker could read the contents of Kernel memory from a user mode process. **Mitigations:** None		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Workarounds: None **Revision:** 1.0 10/08/2019 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1345						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows Server 2016	4519998 Security Update	Important	Information Disclosure	4524152	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1345						
Windows 10 Version 1607 for 32-bit Systems	4519998 Security Update	Important	Information Disclosure	4524152	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4519998 Security Update	Important	Information Disclosure	4524152	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4519998 Security Update	Important	Information Disclosure	4524152	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4520010 Security Update	Important	Information Disclosure	4524151	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version	4520010 Security	Important	Information Disclosure	4524151	Base: 5.5 Temporal: 5	Yes

CVE-2019-1345						
1703 for x64-based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1709 for 32-bit Systems	4520004 Security Update	Important	Information Disclosure	4524150	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4520004 Security Update	Important	Information Disclosure	4524150	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4520008 Security Update	Important	Information Disclosure	4524149	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4520008 Security Update	Important	Information Disclosure	4524149	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1345						
Windows Server, version 1803 (Server Core Installation)	4520008 Security Update	Important	Information Disclosure	4524149	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4520008 Security Update	Important	Information Disclosure	4524149	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4519338 Security Update	Important	Information Disclosure	4524148	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for	4519338 Security Update	Important	Information Disclosure	4524148	Base: 5.5 Temporal: 5 Vector:	Yes

CVE-2019-1345						
x64-based Systems					CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1809 for ARM64-based Systems	4519338 Security Update	Important	Information Disclosure	4524148	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2019	4519338 Security Update	Important	Information Disclosure	4524148	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4519338 Security Update	Important	Information Disclosure	4524148	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-	4520004 Security Update	Important	Information Disclosure	4524150	Base: 5.5 Temporal: 5 Vector:	Yes

CVE-2019-1345						
based Systems					CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1903 for 32-bit Systems	4517389 Security Update	Important	Information Disclosure	4524147	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4517389 Security Update	Important	Information Disclosure	4524147	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4517389 Security Update	Important	Information Disclosure	4524147	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server	4517389 Security Update	Important	Information Disclosure	4524147	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1345						
Core installation)						

CVE-2019-1346 - Windows Denial of Service Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1346 MITRE NVD	**CVE Title:** Windows Denial of Service Vulnerability **Description:** A denial of service vulnerability exists when Windows improperly handles objects in memory. An attacker who successfully exploited the vulnerability could cause a target system to stop responding. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application or to convince a user to open a specific file on a network share. The vulnerability would not allow an attacker to execute code or to elevate user rights directly, but it could be used to cause a target system to stop responding. The update addresses the vulnerability by correcting how Windows handles objects in memory.	Important	Denial of Service

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/08/2019 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1346						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2019-1346						
Windows 7 for 32-bit Systems Service Pack 1	4520003 Security Only 4519976 Monthly Rollup	Important	Denial of Service	4524157	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4519976 Monthly Rollup 4520003 Security Only	Important	Denial of Service	4524157	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4519976 Monthly Rollup 4520003 Security Only	Important	Denial of Service	4524157	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1346						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4519976 Monthly Rollup 4520003 Security Only	Important	Denial of Service	4524157	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4519976 Monthly Rollup 4520003 Security Only	Important	Denial of Service	4524157	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4520002 Monthly Rollup 4520009 Security Only	Important	Denial of Service	4516026	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1346						
Windows Server 2012	4519985 Security Only 4520007 Monthly Rollup	Important	Denial of Service	4524154	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4519985 Security Only 4520007 Monthly Rollup	Important	Denial of Service	4524154	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4519990 Security Only 4520005 Monthly Rollup	Important	Denial of Service	4524156	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1346						
Windows 8.1 for x64-based systems	4519990 Security Only 4520005 Monthly Rollup	Important	Denial of Service	4524156	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4519990 Security Only 4520005 Monthly Rollup	Important	Denial of Service	4524156	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4520005 Monthly Rollup	Important	Denial of Service	4524156	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4519990 Security Only 4520005 Monthly	Important	Denial of Service	4524156	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1346						
	Rollup					
Windows 10 for 32-bit Systems	4520011 Security Update	Important	Denial of Service	4524153	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4520011 Security Update	Important	Denial of Service	4524153	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4519998 Security Update	Important	Denial of Service	4524152	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4519998 Security Update	Important	Denial of Service	4524152	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4519998 Security Update	Important	Denial of Service	4524152	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1346						
Windows Server 2016 (Server Core installation)	4519998 Security Update	Important	Denial of Service	4524152	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4520010 Security Update	Important	Denial of Service	4524151	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4520010 Security Update	Important	Denial of Service	4524151	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4520004 Security Update	Important	Denial of Service	4524150	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4520004 Security Update	Important	Denial of Service	4524150	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1346						
Windows 10 Version 1803 for 32-bit Systems	4520008 Security Update	Important	Denial of Service	4524149	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4520008 Security Update	Important	Denial of Service	4524149	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4520008 Security Update	Important	Denial of Service	4524149	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4520008 Security Update	Important	Denial of Service	4524149	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4519338 Security Update	Important	Denial of Service	4524148	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1346						
Windows 10 Version 1809 for x64-based Systems	4519338 Security Update	Important	Denial of Service	4524148	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4519338 Security Update	Important	Denial of Service	4524148	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4519338 Security Update	Important	Denial of Service	4524148	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4519338 Security Update	Important	Denial of Service	4524148	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4520004 Security Update	Important	Denial of Service	4524150	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1346						
Windows 10 Version 1903 for 32-bit Systems	4517389 Security Update	Important	Denial of Service	4524147	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4517389 Security Update	Important	Denial of Service	4524147	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4517389 Security Update	Important	Denial of Service	4524147	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4517389 Security Update	Important	Denial of Service	4524147	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based	4520002 Monthly Rollup 4520009	Important	Denial of Service	4516026	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1346						
Systems Service Pack 2	Security Only					
Windows Server 2008 for 32-bit Systems Service Pack 2	4520002 Monthly Rollup 4520009 Security Only	Important	Denial of Service	4516026	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4520002 Monthly Rollup 4520009 Security Only	Important	Denial of Service	4516026	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack	4520002 Monthly Rollup 4520009 Security	Important	Denial of Service	4516026	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1346						
2 (Server Core installation)	Only					

CVE-2019-1347 - Windows Denial of Service Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1347 MITRE NVD	**CVE Title:** Windows Denial of Service Vulnerability **Description:** A denial of service vulnerability exists when Windows improperly handles objects in memory. An attacker who successfully exploited the vulnerability could cause a target system to stop responding. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application or to convince a user to open a specific file on a network share. The vulnerability would not allow an attacker to execute code or to elevate user rights directly, but it could be used to cause a target system to stop responding.	Important	Denial of Service

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The update addresses the vulnerability by correcting how Windows handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/08/2019 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1347						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 8.1 for 32-bit systems	4519990 Security Only 4520005 Monthly Rollup	Important	Denial of Service	4524156	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4519990 Security Only 4520005 Monthly Rollup	Important	Denial of Service	4524156	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4519990 Security Only 4520005 Monthly Rollup	Important	Denial of Service	4524156	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1347						
Windows RT 8.1	4520005 Monthly Rollup	Important	Denial of Service	4524156	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4519990 Security Only 4520005 Monthly Rollup	Important	Denial of Service	4524156	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4520011 Security Update	Important	Denial of Service	4524153	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4520011 Security Update	Important	Denial of Service	4524153	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4519998 Security Update	Important	Denial of Service	4524152	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1347						
Windows 10 Version 1607 for 32-bit Systems	4519998 Security Update	Important	Denial of Service	4524152	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4519998 Security Update	Important	Denial of Service	4524152	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4519998 Security Update	Important	Denial of Service	4524152	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4520010 Security Update	Important	Denial of Service	4524151	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4520010 Security Update	Important	Denial of Service	4524151	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1347						
Windows 10 Version 1709 for 32-bit Systems	4520004 Security Update	Important	Denial of Service	4524150	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4520004 Security Update	Important	Denial of Service	4524150	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4520008 Security Update	Important	Denial of Service	4524149	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4520008 Security Update	Important	Denial of Service	4524149	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4520008 Security Update	Important	Denial of Service	4524149	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1347						
Windows 10 Version 1803 for ARM64-based Systems	4520008 Security Update	Important	Denial of Service	4524149	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4519338 Security Update	Important	Denial of Service	4524148	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4519338 Security Update	Important	Denial of Service	4524148	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4519338 Security Update	Important	Denial of Service	4524148	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4519338 Security Update	Important	Denial of Service	4524148	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1347						
Windows Server 2019 (Server Core installation)	4519338 Security Update	Important	Denial of Service	4524148	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4520004 Security Update	Important	Denial of Service	4524150	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4517389 Security Update	Important	Denial of Service	4524147	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4517389 Security Update	Important	Denial of Service	4524147	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4517389 Security Update	Important	Denial of Service	4524147	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1347						
Windows Server, version 1903 (Server Core installation)	4517389 Security Update	Important	Denial of Service	4524147	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1356 - Microsoft Edge based on Edge HTML Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1356 MITRE NVD	**CVE Title:** Microsoft Edge based on Edge HTML Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when Microsoft Edge based on Edge HTML improperly handles objects in memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system. To exploit the vulnerability, in a web-based attack scenario, an attacker could host a website in an attempt to exploit the vulnerability. In addition, compromised websites and websites that accept or host user-provided content could contain specially crafted	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	content that could exploit the vulnerability. However, in all cases an attacker would have no way to force a user to view the attacker-controlled content. Instead, an attacker would have to convince a user to take action. For example, an attacker could trick a user into clicking a link that takes the user to the attacker's site. The update addresses the vulnerability by modifying how Microsoft Edge based on Edge HTML handles objects in memory. **FAQ:** **What type of information could be disclosed by this vulnerability?** The type of information that could be disclosed if an attacker successfully exploited this vulnerability by escaping the sandbox, is the ability to read local files. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/08/2019 07:00:00		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1356						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge (EdgeHTML-based) on Windows Server 2016	4519998 Security Update	Low	Information Disclosure	4524152	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1356						
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1607 for 32-bit Systems	4519998 Security Update	Important	Information Disclosure	4524152	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1607 for x64-based Systems	4519998 Security Update	Important	Information Disclosure	4524152	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version	4520010 Security Update	Important	Information Disclosure	4524151	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1356						
1703 for 32-bit Systems						
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1703 for x64-based Systems	4520010 Security Update	Important	Information Disclosure	4524151	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1709 for 32-bit Systems	4520004 Security Update	Important	Information Disclosure	4524150	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on	4520004 Security	Important	Information Disclosure	4524150	Base: 4.3 Temporal: 3.9 Vector:	Yes

CVE-2019-1356						
Windows 10 Version 1709 for x64-based Systems	Update				CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for 32-bit Systems	4520008 Security Update	Important	Information Disclosure	4524149	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for x64-based Systems	4520008 Security Update	Important	Information Disclosure	4524149	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1356						
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for ARM64-based Systems	4520008 Security Update	Important	Information Disclosure	4524149	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for 32-bit Systems	4519338 Security Update	Important	Information Disclosure	4524148	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10	4519338 Security Update	Important	Information Disclosure	4524148	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1356						
Version 1809 for x64-based Systems						
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for ARM64-based Systems	4519338 Security Update	Important	Information Disclosure	4524148	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows Server 2019	4519338 Security Update	Low	Information Disclosure	4524148	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML	4520004 Security	Important	Information Disclosure	4524150	Base: 4.3 Temporal: 3.9 Vector:	Yes

CVE-2019-1356						
-based) on Windows 10 Version 1709 for ARM64-based Systems	Update				CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for 32-bit Systems	4517389 Security Update	Important	Information Disclosure	4524147	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for	4517389 Security Update	Important	Information Disclosure	4524147	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1356						
x64-based Systems						
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for ARM64-based Systems	4517389 Security Update	Important	Information Disclosure	4524147	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1357 - Microsoft Browser Spoofing Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1357	**CVE Title:** Microsoft Browser Spoofing Vulnerability **Description:**	Important	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	A spoofing vulnerability exists when Microsoft Browsers improperly handle browser cookies. An attacker who successfully exploited this vulnerability could trick a browser into overwriting a secure cookie with an insecure cookie. The insecure cookie could serve as a pivot to chain an attack with other vulnerabilities in web services. To exploit the vulnerability, the user must either browse to a malicious website or be redirected to it. In an email attack scenario, an attacker could send an email message in an attempt to convince the user to click a link to a malicious site. In a web-based attack scenario, an attacker could host a specially crafted website designed to appear as a legitimate website to the user. However, the attacker would have no way to force the user to visit the specially crafted website. The attacker would have to convince the user to visit the specially crafted website, typically by way of enticement in an email or instant message. The security update addresses the vulnerability by correcting how Microsoft Browsers handle browser cookies. **FAQ:** None **Mitigations:** None **Workarounds:**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 10/08/2019 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1357						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1	4519974 IE Cumulative 4519976 Monthly Rollup	Important	Spoofing	4524157	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes

CVE-2019-1357						
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1	4519974 IE Cumulative 4519976 Monthly Rollup	Important	Spoofing	4524157	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4519974 IE Cumulative 4519976 Monthly Rollup	Low	Spoofing	4524157	Base: 3.5 Temporal: 3.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes
Internet Explorer 11 on Windows Server 2012	4519974 IE Cumulative	Low	Spoofing	4524135	Base: 3.5 Temporal: 3.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4519974 IE Cumulative 4520005 Monthly Rollup	Important	Spoofing	4524156	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes

CVE-2019-1357						
Internet Explorer 11 on Windows 8.1 for x64-based systems	4519974 IE Cumulative 4520005 Monthly Rollup	Important	Spoofing	4524156	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes
Internet Explorer 11 on Windows Server 2012 R2	4519974 IE Cumulative 4520005 Monthly Rollup	Low	Spoofing	4524156	Base: 3.5 Temporal: 3.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes
Internet Explorer 11 on Windows RT 8.1	4520005 Monthly Rollup	Important	Spoofing	4524156	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes
Internet Explorer 11 on Windows 10 for 32-bit Systems	4520011 Security Update	Important	Spoofing	4524153	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes
Internet Explorer 11 on	4520011 Security	Important	Spoofing	4524153	Base: 5.4 Temporal: 4.9	Yes

CVE-2019-1357						
Windows 10 for x64-based Systems	Update				Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	
Internet Explorer 11 on Windows Server 2016	4519998 Security Update	Low	Spoofing	4524152	Base: 3.5 Temporal: 3.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems	4519998 Security Update	Important	Spoofing	4524152	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4519998 Security Update	Important	Spoofing	4524152	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes
Internet Explorer 11 on Windows 10 Version 1703	4520010 Security Update	Important	Spoofing	4524151	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes

CVE-2019-1357						
for 32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems	4520010 Security Update	Important	Spoofing	4524151	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems	4520004 Security Update	Important	Spoofing	4524150	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems	4520004 Security Update	Important	Spoofing	4524150	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes
Internet Explorer 11 on Windows 10	4520008 Security	Important	Spoofing	4524149	Base: 5.4 Temporal: 4.9	Yes

CVE-2019-1357						
Version 1803 for 32-bit Systems	Update				Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems	4520008 Security Update	Important	Spoofing	4524149	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes
Internet Explorer 11 on Windows 10 Version 1803 for ARM64-based Systems	4520008 Security Update	Important	Spoofing	4524149	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes
Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems	4519338 Security Update	Important	Spoofing	4524148	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes
Internet Explorer 11 on	4519338 Security	Important	Spoofing	4524148	Base: 5.4 Temporal: 4.9	Yes

CVE-2019-1357						
Windows 10 Version 1809 for x64-based Systems	Update				Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	
Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems	4519338 Security Update	Important	Spoofing	4524148	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes
Internet Explorer 11 on Windows Server 2019	4519338 Security Update	Low	Spoofing	4524148	Base: 3.5 Temporal: 3.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes
Internet Explorer 11 on Windows 10 Version 1709 for ARM64-based Systems	4520004 Security Update	Important	Spoofing	4524150	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes
Internet Explorer 11 on Windows 10	4517389 Security	Important	Spoofing	4524147	Base: 5.4 Temporal: 4.9	Yes

CVE-2019-1357						
Version 1903 for 32-bit Systems	Update				Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	
Internet Explorer 11 on Windows 10 Version 1903 for x64-based Systems	4517389 Security Update	Important	Spoofing	4524147	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes
Internet Explorer 11 on Windows 10 Version 1903 for ARM64-based Systems	4517389 Security Update	Important	Spoofing	4524147	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes
Internet Explorer 10 on Windows Server 2012	4520007 Monthly Rollup 4519974 IE Cumulative	Low	Spoofing	4524135	Base: 3.5 Temporal: 3.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes
Microsoft Edge	4520008 Security	Important	Spoofing	4524149	Base: 5.4 Temporal: 4.9	Yes

CVE-2019-1357						
(EdgeHTML-based) on Windows 10 Version 1803 for 32-bit Systems	Update				Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for x64-based Systems	4520008 Security Update	Important	Spoofing	4524149	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for ARM64-based Systems	4520008 Security Update	Important	Spoofing	4524149	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes

CVE-2019-1357						
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for 32-bit Systems	4519338 Security Update	Important	Spoofing	4524148	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for x64-based Systems	4519338 Security Update	Important	Spoofing	4524148	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809	4519338 Security Update	Important	Spoofing	4524148	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes

CVE-2019-1357						
for ARM64-based Systems						
Microsoft Edge (EdgeHTML-based) on Windows Server 2019	4519338 Security Update	Important	Spoofing	4524148	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for 32-bit Systems	4517389 Security Update	Important	Spoofing	4524147	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903	4517389 Security Update	Important	Spoofing	4524147	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes

CVE-2019-1357						
for x64-based Systems						
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for ARM64-based Systems	4517389 Security Update	Important	Spoofing	4524147	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes

CVE-2019-1358 - Jet Database Engine Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1358	**CVE Title:** Jet Database Engine Remote Code Execution Vulnerability **Description:**	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory. An attacker who successfully exploited this vulnerability could execute arbitrary code on a victim system. An attacker could exploit this vulnerability by enticing a victim to open a specially crafted file. The update addresses the vulnerability by correcting the way the Windows Jet Database Engine handles objects in memory. **FAQ:** **Are Active Directory and Exchange Server affected by this vulnerability?** No, Active Directory and Exchange Server are not affected. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/08/2019 07:00:00 Information published.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1358						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4520003 Security Only 4519976 Monthly Rollup	Important	Remote Code Execution	4524157	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems	4519976 Monthly Rollup 4520003 Security	Important	Remote Code Execution	4524157	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1358						
Service Pack 1	Only					
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4519976 Monthly Rollup 4520003 Security Only	Important	Remote Code Execution	4524157	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4519976 Monthly Rollup 4520003 Security Only	Important	Remote Code Execution	4524157	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-	4519976 Monthly Rollup	Important	Remote Code Execution	4524157	Base: 7.8 Temporal: 7	Yes

CVE-2019-1358						
based Systems Service Pack 1	4520003 Security Only				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4520002 Monthly Rollup 4520009 Security Only	Important	Remote Code Execution	4516026	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012	4519985 Security Only 4520007 Monthly Rollup	Important	Remote Code Execution	4524154	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server	4519985 Security Only	Important	Remote Code Execution	4524154	Base: 7.8 Temporal: 7	Yes

CVE-2019-1358						
Core installation)	4520007 Monthly Rollup				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 8.1 for 32-bit systems	4519990 Security Only 4520005 Monthly Rollup	Important	Remote Code Execution	4524156	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4519990 Security Only 4520005 Monthly Rollup	Important	Remote Code Execution	4524156	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4519990 Security Only 4520005 Monthly	Important	Remote Code Execution	4524156	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1358						
	Rollup					
Windows RT 8.1	4520005 Monthly Rollup	Important	Remote Code Execution	4524156	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4519990 Security Only 4520005 Monthly Rollup	Important	Remote Code Execution	4524156	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4520011 Security Update	Important	Remote Code Execution	4524153	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4520011 Security Update	Important	Remote Code Execution	4524153	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1358						
Windows Server 2016	4519998 Security Update	Important	Remote Code Execution	4524152	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4519998 Security Update	Important	Remote Code Execution	4524152	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4519998 Security Update	Important	Remote Code Execution	4524152	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4519998 Security Update	Important	Remote Code Execution	4524152	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for	4520010 Security Update	Important	Remote Code Execution	4524151	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1358						
32-bit Systems						
Windows 10 Version 1703 for x64-based Systems	4520010 Security Update	Important	Remote Code Execution	4524151	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4520004 Security Update	Important	Remote Code Execution	4524150	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4520004 Security Update	Important	Remote Code Execution	4524150	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4520008 Security Update	Important	Remote Code Execution	4524149	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1358						
Windows 10 Version 1803 for x64-based Systems	4520008 Security Update	Important	Remote Code Execution	4524149	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4520008 Security Update	Important	Remote Code Execution	4524149	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4520008 Security Update	Important	Remote Code Execution	4524149	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4519338 Security Update	Important	Remote Code Execution	4524148	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1358						
Windows 10 Version 1809 for x64-based Systems	4519338 Security Update	Important	Remote Code Execution	4524148	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4519338 Security Update	Important	Remote Code Execution	4524148	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4519338 Security Update	Important	Remote Code Execution	4524148	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4519338 Security Update	Important	Remote Code Execution	4524148	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for	4520004 Security	Important	Remote Code Execution	4524150	Base: 7.8 Temporal: 7	Yes

CVE-2019-1358						
ARM64-based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1903 for 32-bit Systems	4517389 Security Update	Important	Remote Code Execution	4524147	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4517389 Security Update	Important	Remote Code Execution	4524147	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4517389 Security Update	Important	Remote Code Execution	4524147	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903	4517389 Security Update	Important	Remote Code Execution	4524147	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1358						
(Server Core installation)						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4520002 Monthly Rollup 4520009 Security Only	Important	Remote Code Execution	4516026	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4520002 Monthly Rollup 4520009 Security Only	Important	Remote Code Execution	4516026	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems	4520002 Monthly Rollup 4520009 Security	Important	Remote Code Execution	4516026	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1358						
Service Pack 2	Only					
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4520002 Monthly Rollup 4520009 Security Only	Important	Remote Code Execution	4516026	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1359 - Jet Database Engine Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-	**CVE Title:** Jet Database Engine Remote Code Execution Vulnerability **Description:**	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
1359 MITRE NVD	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory. An attacker who successfully exploited this vulnerability could execute arbitrary code on a victim system. An attacker could exploit this vulnerability by enticing a victim to open a specially crafted file. The update addresses the vulnerability by correcting the way the Windows Jet Database Engine handles objects in memory. **FAQ:** **Are Active Directory and Exchange Server affected by this vulnerability?** No, Active Directory and Exchange Server are not affected. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/08/2019 07:00:00 Information published.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1359						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4520003 Security Only 4519976 Monthly Rollup	Important	Remote Code Execution	4524157	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems	4519976 Monthly Rollup 4520003 Security	Important	Remote Code Execution	4524157	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1359						
Service Pack 1	Only					
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4519976 Monthly Rollup 4520003 Security Only	Important	Remote Code Execution	4524157	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4519976 Monthly Rollup 4520003 Security Only	Important	Remote Code Execution	4524157	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-	4519976 Monthly Rollup	Important	Remote Code Execution	4524157	Base: 7.8 Temporal: 7	Yes

CVE-2019-1359						
based Systems Service Pack 1	4520003 Security Only				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4520002 Monthly Rollup 4520009 Security Only	Important	Remote Code Execution	4516026	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012	4519985 Security Only 4520007 Monthly Rollup	Important	Remote Code Execution	4524154	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server	4519985 Security Only	Important	Remote Code Execution	4524154	Base: 7.8 Temporal: 7	Yes

CVE-2019-1359						
Core installation)	4520007 Monthly Rollup				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 8.1 for 32-bit systems	4519990 Security Only 4520005 Monthly Rollup	Important	Remote Code Execution	4524156	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4519990 Security Only 4520005 Monthly Rollup	Important	Remote Code Execution	4524156	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4519990 Security Only 4520005 Monthly	Important	Remote Code Execution	4524156	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1359						
	Rollup					
Windows RT 8.1	4520005 Monthly Rollup	Important	Remote Code Execution	4524156	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4519990 Security Only 4520005 Monthly Rollup	Important	Remote Code Execution	4524156	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4520011 Security Update	Important	Remote Code Execution	4524153	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4520011 Security Update	Important	Remote Code Execution	4524153	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1359						
Windows Server 2016	4519998 Security Update	Important	Remote Code Execution	4524152	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4519998 Security Update	Important	Remote Code Execution	4524152	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4519998 Security Update	Important	Remote Code Execution	4524152	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4519998 Security Update	Important	Remote Code Execution	4524152	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for	4520010 Security Update	Important	Remote Code Execution	4524151	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1359						
32-bit Systems						
Windows 10 Version 1703 for x64-based Systems	4520010 Security Update	Important	Remote Code Execution	4524151	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4520004 Security Update	Important	Remote Code Execution	4524150	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4520004 Security Update	Important	Remote Code Execution	4524150	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4520008 Security Update	Important	Remote Code Execution	4524149	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1359						
Windows 10 Version 1803 for x64-based Systems	4520008 Security Update	Important	Remote Code Execution	4524149	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4520008 Security Update	Important	Remote Code Execution	4524149	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4520008 Security Update	Important	Remote Code Execution	4524149	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4519338 Security Update	Important	Remote Code Execution	4524148	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1359						
Windows 10 Version 1809 for x64-based Systems	4519338 Security Update	Important	Remote Code Execution	4524148	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4519338 Security Update	Important	Remote Code Execution	4524148	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4519338 Security Update	Important	Remote Code Execution	4524148	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4519338 Security Update	Important	Remote Code Execution	4524148	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for	4520004 Security	Important	Remote Code Execution	4524150	Base: 7.8 Temporal: 7	Yes

CVE-2019-1359						
ARM64-based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1903 for 32-bit Systems	4517389 Security Update	Important	Remote Code Execution	4524147	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4517389 Security Update	Important	Remote Code Execution	4524147	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4517389 Security Update	Important	Remote Code Execution	4524147	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903	4517389 Security Update	Important	Remote Code Execution	4524147	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1359						
(Server Core installation)						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4520002 Monthly Rollup 4520009 Security Only	Important	Remote Code Execution	4516026	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4520002 Monthly Rollup 4520009 Security Only	Important	Remote Code Execution	4516026	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems	4520002 Monthly Rollup 4520009 Security	Important	Remote Code Execution	4516026	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1359						
Service Pack 2	Only					
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4520002 Monthly Rollup 4520009 Security Only	Important	Remote Code Execution	4516026	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1361 - Microsoft Graphics Components Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1361 MITRE NVD	**CVE Title:** Microsoft Graphics Components Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists in the way that Microsoft Graphics Components handle objects in memory. An attacker who successfully exploited the vulnerability could obtain information that could be useful for further exploitation. To exploit the vulnerability, a user would have to open a specially crafted file. The security update addresses the vulnerability by correcting how Microsoft Graphics Components handle objects in memory. **FAQ:** **What type of information could be disclosed by this vulnerability?** The type of information that could be disclosed if an attacker successfully exploited this vulnerability is uninitialized memory.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 10/08/2019 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1361						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2019-1361						
Windows 7 for 32-bit Systems Service Pack 1	4520003 Security Only 4519976 Monthly Rollup	Important	Information Disclosure	4524157	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4519976 Monthly Rollup 4520003 Security Only	Important	Information Disclosure	4524157	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server	4519976 Monthly Rollup 4520003 Security Only	Important	Information Disclosure	4524157	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1361						
Core installation)						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4519976 Monthly Rollup 4520003 Security Only	Important	Information Disclosure	4524157	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4519976 Monthly Rollup 4520003 Security Only	Important	Information Disclosure	4524157	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1362 - Win32k Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1362 MITRE NVD	**CVE Title:** Win32k Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. The update addresses this vulnerability by correcting how the Windows kernel-mode driver handles objects in memory. **FAQ:** None **Mitigations:** None	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Workarounds: None **Revision:** 1.0 10/08/2019 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1362						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4520003 Security Only 4519976 Monthly	Important	Elevation of Privilege	4524157	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1362						
	Rollup					
Windows 7 for x64-based Systems Service Pack 1	4519976 Monthly Rollup 4520003 Security Only	Important	Elevation of Privilege	4524157	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4519976 Monthly Rollup 4520003 Security Only	Important	Elevation of Privilege	4524157	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-	4519976 Monthly Rollup 4520003	Important	Elevation of Privilege	4524157	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1362						
Based Systems Service Pack 1	Security Only					
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4519976 Monthly Rollup 4520003 Security Only	Important	Elevation of Privilege	4524157	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4520002 Monthly Rollup 4520009 Security Only	Important	Elevation of Privilege	4516026	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-	4520002 Monthly Rollup	Important	Elevation of Privilege	4516026	Base: 7 Temporal: 6.3	Yes

CVE-2019-1362						
Based Systems Service Pack 2	4520009 Security Only				Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2008 for 32-bit Systems Service Pack 2	4520002 Monthly Rollup 4520009 Security Only	Important	Elevation of Privilege	4516026	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4520002 Monthly Rollup 4520009 Security Only	Important	Elevation of Privilege	4516026	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems	4520002 Monthly Rollup 4520009 Security	Important	Elevation of Privilege	4516026	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1362						
Service Pack 2 (Server Core installation)	Only					

CVE-2019-1363 - Windows GDI Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1363 MITRE NVD	**CVE Title:** Windows GDI Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, allowing an attacker to retrieve information from a targeted system. By itself, the information disclosure does not allow arbitrary code execution; however, it could allow arbitrary code to be run if the attacker uses it in combination with another vulnerability. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by correcting how GDI handles memory addresses. **FAQ:** **What type of information could be disclosed by this vulnerability?** The type of information that could be disclosed if an attacker successfully exploited this vulnerability is the contents of Kernel memory. An attacker could read the contents of Kernel memory from a user mode process. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/08/2019 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1363						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4520003 Security Only 4519976 Monthly Rollup	Important	Information Disclosure	4524157	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4519976 Monthly Rollup 4520003 Security Only	Important	Information Disclosure	4524157	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server	4519976 Monthly	Important	Information Disclosure	4524157	Base: 5.5 Temporal: 5	Yes

CVE-2019-1363						
2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	Rollup 4520003 Security Only				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4519976 Monthly Rollup 4520003 Security Only	Important	Information Disclosure	4524157	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4519976 Monthly Rollup 4520003 Security Only	Important	Information Disclosure	4524157	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1364 - Win32k Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1364 MITRE NVD	**CVE Title:** Win32k Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. The update addresses this vulnerability by correcting how the Windows kernel-mode driver handles objects in memory. **FAQ:** None **Mitigations:** None	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Workarounds: None **Revision:** 1.0 10/08/2019 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1364						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4520003 Security Only 4519976 Monthly	Important	Elevation of Privilege	4524157	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1364						
	Rollup					
Windows 7 for x64-based Systems Service Pack 1	4519976 Monthly Rollup 4520003 Security Only	Important	Elevation of Privilege	4524157	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4519976 Monthly Rollup 4520003 Security Only	Important	Elevation of Privilege	4524157	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-	4519976 Monthly Rollup 4520003	Important	Elevation of Privilege	4524157	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1364						
Based Systems Service Pack 1	Security Only					
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4519976 Monthly Rollup 4520003 Security Only	Important	Elevation of Privilege	4524157	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4520002 Monthly Rollup 4520009 Security Only	Important	Elevation of Privilege	4516026	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-	4520002 Monthly Rollup	Important	Elevation of Privilege	4516026	Base: 7 Temporal: 6.3	Yes

CVE-2019-1364						
Based Systems Service Pack 2	4520009 Security Only				Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2008 for 32-bit Systems Service Pack 2	4520002 Monthly Rollup 4520009 Security Only	Important	Elevation of Privilege	4516026	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4520002 Monthly Rollup 4520009 Security Only	Important	Elevation of Privilege	4516026	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems	4520002 Monthly Rollup 4520009 Security	Important	Elevation of Privilege	4516026	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1364						
Service Pack 2 (Server Core installation)	Only					

CVE-2019-1365 - Microsoft IIS Server Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1365 MITRE NVD	**CVE Title:** Microsoft IIS Server Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when Microsoft IIS Server fails to check the length of a buffer prior to copying memory to it. An attacker who successfully exploited this vulnerability can allow an unprivileged function ran by the user to execute code in the context of NT AUTHORITY\system escaping the Sandbox. The security update addresses the vulnerability by correcting how Microsoft IIS Server sanitizes web requests.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/08/2019 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1365						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2019-1365						
Windows 7 for 32-bit Systems Service Pack 1	4520003 Security Only 4519976 Monthly Rollup	Important	Elevation of Privilege	4524157	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4519976 Monthly Rollup 4520003 Security Only	Important	Elevation of Privilege	4524157	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server	4519976 Monthly Rollup 4520003 Security Only	Important	Elevation of Privilege	4524157	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1365						
Core installation)						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4519976 Monthly Rollup 4520003 Security Only	Important	Elevation of Privilege	4524157	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4519976 Monthly Rollup 4520003 Security Only	Important	Elevation of Privilege	4524157	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4520002 Monthly Rollup 4520009 Security	Important	Elevation of Privilege	4516026	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1365						
(Server Core installation)	Only					
Windows Server 2012	4519985 Security Only 4520007 Monthly Rollup	Important	Elevation of Privilege	4524154	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4519985 Security Only 4520007 Monthly Rollup	Important	Elevation of Privilege	4524154	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4519990 Security Only 4520005 Monthly	Important	Elevation of Privilege	4524156	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1365						
	Rollup					
Windows 8.1 for x64-based systems	4519990 Security Only 4520005 Monthly Rollup	Important	Elevation of Privilege	4524156	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4519990 Security Only 4520005 Monthly Rollup	Important	Elevation of Privilege	4524156	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4520005 Monthly Rollup	Important	Elevation of Privilege	4524156	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server	4519990 Security Only	Important	Elevation of Privilege	4524156	Base: 7.5 Temporal: 6.7	Yes

CVE-2019-1365						
Core installation)	4520005 Monthly Rollup				Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2016	4519998 Security Update	Important	Elevation of Privilege	4524152	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4519998 Security Update	Important	Elevation of Privilege	4524152	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4519998 Security Update	Important	Elevation of Privilege	4524152	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4519998 Security Update	Important	Elevation of Privilege	4524152	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1365						
Windows 10 Version 1803 for 32-bit Systems	4520008 Security Update	Important	Elevation of Privilege	4524149	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4520008 Security Update	Important	Elevation of Privilege	4524149	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4520008 Security Update	Important	Elevation of Privilege	4524149	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4520008 Security Update	Important	Elevation of Privilege	4524149	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1365						
Windows 10 Version 1809 for 32-bit Systems	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4519338 Security Update	Important	Elevation of Privilege	4524148	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server	4519338 Security	Important	Elevation of Privilege	4524148	Base: 7.5 Temporal: 6.7	Yes

CVE-2019-1365						
Core installation)	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1903 for 32-bit Systems	4517389 Security Update	Important	Elevation of Privilege	4524147	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4517389 Security Update	Important	Elevation of Privilege	4524147	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4517389 Security Update	Important	Elevation of Privilege	4524147	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server	4517389 Security Update	Important	Elevation of Privilege	4524147	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1365						
Core installation)						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4520002 Monthly Rollup 4520009 Security Only	Important	Elevation of Privilege	4516026	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4520002 Monthly Rollup 4520009 Security Only	Important	Elevation of Privilege	4516026	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems	4520002 Monthly Rollup 4520009 Security	Important	Elevation of Privilege	4516026	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1365						
Service Pack 2	Only					
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4520002 Monthly Rollup 4520009 Security Only	Important	Elevation of Privilege	4516026	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1366 - Chakra Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1366 MITRE NVD	**CVE Title:** Chakra Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by modifying how the Chakra scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/08/2019 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1366						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge (EdgeHTML-based) on Windows 10 for 32-bit Systems	4520011 Security Update	Critical	Remote Code Execution	4524153	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 for x64-based Systems	4520011 Security Update	Critical	Remote Code Execution	4524153	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows Server 2016	4519998 Security Update	Moderate	Remote Code Execution	4524152	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1366						
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1607 for 32-bit Systems	4519998 Security Update	Critical	Remote Code Execution	4524152	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1607 for x64-based Systems	4519998 Security Update	Critical	Remote Code Execution	4524152	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version	4520010 Security Update	Critical	Remote Code Execution	4524151	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1366						
1703 for 32-bit Systems						
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1703 for x64-based Systems	4520010 Security Update	Critical	Remote Code Execution	4524151	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1709 for 32-bit Systems	4520004 Security Update	Critical	Remote Code Execution	4524150	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on	4520004 Security Update	Critical	Remote Code Execution	4524150	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1366						
Windows 10 Version 1709 for x64-based Systems						
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for 32-bit Systems	4520008 Security Update	Critical	Remote Code Execution	4524149	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for x64-based Systems	4520008 Security Update	Critical	Remote Code Execution	4524149	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1366						
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for ARM64-based Systems	4520008 Security Update	Critical	Remote Code Execution	4524149	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for 32-bit Systems	4519338 Security Update	Critical	Remote Code Execution	4524148	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10	4519338 Security Update	Critical	Remote Code Execution	4524148	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1366						
Version 1809 for x64-based Systems						
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for ARM64-based Systems	4519338 Security Update	Critical	Remote Code Execution	4524148	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows Server 2019	4519338 Security Update	Moderate	Remote Code Execution	4524148	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-	4520004 Security	Critical	Remote Code Execution	4524150	Base: 4.2 Temporal: 3.8	Yes

CVE-2019-1366						
based) on Windows 10 Version 1709 for ARM64-based Systems	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for 32-bit Systems	4517389 Security Update	Critical	Remote Code Execution	4524147	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for	4517389 Security Update	Critical	Remote Code Execution	4524147	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1366						
x64-based Systems						
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for ARM64-based Systems	4517389 Security Update	Critical	Remote Code Execution	4524147	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
ChakraCore	Release Notes Security Update	Critical	Remote Code Execution	4524147	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Maybe

CVE-2019-1368 - Windows Secure Boot Security Feature Bypass Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1368 MITRE NVD	**CVE Title:** Windows Secure Boot Security Feature Bypass Vulnerability **Description:** A security feature bypass exists when Windows Secure Boot improperly restricts access to debugging functionality. An attacker who successfully exploited this vulnerability could disclose protected kernel memory. To exploit the vulnerability, an attacker must gain physical access to the target system prior to the next system reboot. The security update addresses the vulnerability by preventing access to certain debugging options when Windows Secure Boot is enabled. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Security Feature Bypass

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 10/08/2019 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1368						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4520008 Security Update	Important	Security Feature Bypass	4524149	Base: 4.9 Temporal: 4.4 Vector: CVSS:3.0/AV:P/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1368						
Windows 10 Version 1803 for x64-based Systems	4520008 Security Update	Important	Security Feature Bypass	4524149	Base: 4.9 Temporal: 4.4 Vector: CVSS:3.0/AV:P/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4520008 Security Update	Important	Security Feature Bypass	4524149	Base: 4.9 Temporal: 4.4 Vector: CVSS:3.0/AV:P/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4520008 Security Update	Important	Security Feature Bypass	4524149	Base: 4.9 Temporal: 4.4 Vector: CVSS:3.0/AV:P/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4519338 Security Update	Important	Security Feature Bypass	4524148	Base: 4.9 Temporal: 4.4 Vector: CVSS:3.0/AV:P/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1368						
Windows 10 Version 1809 for x64-based Systems	4519338 Security Update	Important	Security Feature Bypass	4524148	Base: 4.9 Temporal: 4.4 Vector: CVSS:3.0/AV:P/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4519338 Security Update	Important	Security Feature Bypass	4524148	Base: 4.9 Temporal: 4.4 Vector: CVSS:3.0/AV:P/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2019	4519338 Security Update	Important	Security Feature Bypass	4524148	Base: 4.9 Temporal: 4.4 Vector: CVSS:3.0/AV:P/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4519338 Security Update	Important	Security Feature Bypass	4524148	Base: 4.9 Temporal: 4.4 Vector: CVSS:3.0/AV:P/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for	4517389 Security Update	Important	Security Feature Bypass	4524147	Base: 4.9 Temporal: 4.4 Vector: CVSS:3.0/AV:P/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1368						
32-bit Systems						
Windows 10 Version 1903 for x64-based Systems	4517389 Security Update	Important	Security Feature Bypass	4524147	Base: 4.9 Temporal: 4.4 Vector: CVSS:3.0/AV:P/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4517389 Security Update	Important	Security Feature Bypass	4524147	Base: 4.9 Temporal: 4.4 Vector: CVSS:3.0/AV:P/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4517389 Security Update	Important	Security Feature Bypass	4524147	Base: 4.9 Temporal: 4.4 Vector: CVSS:3.0/AV:P/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1369 - Open Enclave SDK Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1369 MITRE NVD	**CVE Title:** Open Enclave SDK Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when affected Open Enclave SDK versions improperly handle objects in memory. An attacker who successfully exploited this vulnerability could obtain information stored in the Enclave. To exploit this vulnerability, an attacker would have to successfully compromise the host application running the enclave. The attacker can then pivot to the enclave and exploit this vulnerability without user interaction. The security update addresses the vulnerability by modifying how Open Enclave SDK handle objects in memory. **FAQ:** **What type of information could be disclosed by this vulnerability?**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The type of information that could be disclosed if an attacker successfully exploited this vulnerability is Enclave memory read - unprivileged write to enclave memory from a host application, which can leak memory contents of the enclave. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/08/2019 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1369						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Open Enclave SDK	Release Notes Security Update	Important	Information Disclosure		Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1371 - Internet Explorer Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1371 MITRE NVD	**CVE Title:** Internet Explorer Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, the attacker could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	An attacker could host a specially crafted website designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website. The attacker could also take advantage of compromised websites, or websites that accept or host user-provided content or advertisements, by adding specially crafted content that could exploit the vulnerability. However, in all cases an attacker would have no way to force a user to view the attacker-controlled content. Instead, an attacker would have to convince a user to take action, typically by an enticement in an email or instant message, or by getting the user to open an attachment sent through email. The security update addresses the vulnerability by modifying how Internet Explorer handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/08/2019 07:00:00 Information published.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1371						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2	4519974 IE Cumulative 4520002 Monthly Rollup	Low	Remote Code Execution	4516026	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1371						
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2	4519974 IE Cumulative 4520002 Monthly Rollup	Low	Remote Code Execution	4516026	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1	4519974 IE Cumulative 4519976 Monthly Rollup	Important	Remote Code Execution	4524157	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on	4519974 IE Cumulative 4519976	Important	Remote Code Execution	4524157	Base: 7.5 Temporal: 6.7	Yes

CVE-2019-1371						
Windows 7 for x64-based Systems Service Pack 1	Monthly Rollup				Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4519974 IE Cumulative 4519976 Monthly Rollup	Low	Remote Code Execution	4524157	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows	4519974 IE Cumulative	Low	Remote Code Execution	4524135	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1371						
Server 2012						
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4519974 IE Cumulative 4520005 Monthly Rollup	Important	Remote Code Execution	4524156	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 8.1 for x64-based systems	4519974 IE Cumulative 4520005 Monthly Rollup	Important	Remote Code Execution	4524156	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2012 R2	4519974 IE Cumulative 4520005 Monthly Rollup	Low	Remote Code Execution	4524156	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1371						
Internet Explorer 11 on Windows RT 8.1	4520005 Monthly Rollup	Important	Remote Code Execution	4524156	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 for 32-bit Systems	4520011 Security Update	Important	Remote Code Execution	4524153	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 for x64-based Systems	4520011 Security Update	Important	Remote Code Execution	4524153	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on	4519998 Security	Low	Remote Code Execution	4524152	Base: 6.4 Temporal: 5.8	Yes

CVE-2019-1371						
Windows Server 2016	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems	4519998 Security Update	Important	Remote Code Execution	4524152	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4519998 Security Update	Important	Remote Code Execution	4524152	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1371						
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems	4520010 Security Update	Important	Remote Code Execution	4524151	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems	4520010 Security Update	Important	Remote Code Execution	4524151	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows	4520004 Security Update	Important	Remote Code Execution	4524150	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1371						
10 Version 1709 for 32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems	4520004 Security Update	Important	Remote Code Execution	4524150	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1803 for	4520008 Security Update	Important	Remote Code Execution	4524149	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1371						
32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems	4520008 Security Update	Important	Remote Code Execution	4524149	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1803 for ARM64-based Systems	4520008 Security Update	Important	Remote Code Execution	4524149	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1371						
Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems	4519338 Security Update	Important	Remote Code Execution	4524148	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems	4519338 Security Update	Important	Remote Code Execution	4524148	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows	4519338 Security Update	Important	Remote Code Execution	4524148	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1371						
10 Version 1809 for ARM64-based Systems						
Internet Explorer 11 on Windows Server 2019	4519338 Security Update	Low	Remote Code Execution	4524148	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1709 for ARM64-based Systems	4520004 Security Update	Important	Remote Code Execution	4524150	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1371						
Internet Explorer 11 on Windows 10 Version 1903 for 32-bit Systems	4517389 Security Update	Important	Remote Code Execution	4524147	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1903 for x64-based Systems	4517389 Security Update	Important	Remote Code Execution	4524147	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows	4517389 Security Update	Important	Remote Code Execution	4524147	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1371						
10 Version 1903 for ARM64-based Systems						
Internet Explorer 10 on Windows Server 2012	4520007 Monthly Rollup 4519974 IE Cumulative	Low	Remote Code Execution	4524135	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1372 - Azure App Service Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-	**CVE Title:** Azure App Service Remote Code Execution Vulnerability **Description:**	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
1372 MITRE NVD	An remote code execution vulnerability exists when Azure App Service/ Antares on Azure Stack fails to check the length of a buffer prior to copying memory to it. An attacker who successfully exploited this vulnerability could allow an unprivileged function run by the user to execute code in the context of NT AUTHORITY\system thereby escaping the Sandbox. The security update addresses the vulnerability by ensuring that Azure App Service sanitizes user inputs. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/08/2019 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1372						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Azure App Service on Azure Stack	Release Notes Security Update	Critical	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1375 - Microsoft Dynamics 365 (On-Premise) Cross Site Scripting Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-	**CVE Title:** Microsoft Dynamics 365 (On-Premise) Cross Site Scripting Vulnerability **Description:**	Important	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
1375 MITRE NVD	A cross site scripting vulnerability exists when Microsoft Dynamics 365 (on-premises) does not properly sanitize a specially crafted web request to an affected Dynamics server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected Dynamics server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current authenticated user. These attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions within Dynamics Server on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that Dynamics Server properly sanitizes web requests. **FAQ:** None **Mitigations:** None **Workarounds:** None		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 10/08/2019 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1375						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Dynamics 365 (on-premises) version 9.0	4515519 Security Update	Important	Spoofing		Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1376 - SQL Server Management Studio Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1376 MITRE NVD	**CVE Title:** SQL Server Management Studio Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists in Microsoft SQL Server Management Studio (SSMS) when it improperly enforces permissions. An attacker could exploit the vulnerability if the attacker's credentials allow access to an affected SQL server database. An attacker who successfully exploited the vulnerability could gain additional database and file information. The security update addresses the vulnerability by correcting how SQL Server Management Studio enforces permissions. **FAQ:** **What type of information could be disclosed by this vulnerability?**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The type of information that could be disclosed if an attacker successfully exploited this vulnerability relates to SQL table columns that would normally be restricted. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/08/2019 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1376						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
SQL Server Management Studio 18.3.1	Release Notes Security Update	Important	Information Disclosure		Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1378 - Windows 10 Update Assistant Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1378 MITRE NVD	**CVE Title:** Windows 10 Update Assistant Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in Windows 10 Update Assistant in the way it handles permissions.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	A locally authenticated attacker could run arbitrary code with elevated system privileges. After successfully exploiting the vulnerability, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. The security update addresses the vulnerability by ensuring the Windows 10 Update Assistant properly handles permissions. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/08/2019 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2019-1378						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows Update Assistant	Update pending	Important	Elevation of Privilege		Base: N/A Temporal: N/A Vector: N/A	Maybe

北京神州绿盟信息安全科技股份有限公司（简称绿盟科技）成立于 2000 年 4 月，总部位于北京。在国内外设有 30 多个分支机构，为政府、运营商、金融、能源、互联网以及教育、医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。

基于多年的安全攻防研究，绿盟科技在网络及终端安全、互联网基础安全、合规及安全管理等领域，为客户提供入侵检测/防护、抗拒绝服务攻击、远程安全评估以及 Web 安全防护等产品以及专业安全服务。

北京神州绿盟信息安全科技股份有限公司于 2014 年 1 月 29 日起在深圳证券交易所创业板上市，股票简称：绿盟科技，股票代码：300369。

绿盟科技官方微博二维码

绿盟科技官方微信二维码