微软发布 7 月补丁修复 79 个安全问题

安全威胁通告

发布时间：2019 年 7 月 10 日

综述

微软于周二发布了 7 月安全更新补丁，修复了 79 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.NET Framework、ASP.NET、Azure、Azure DevOps、Internet Explorer、Microsoft Browsers、Microsoft Exchange Server、Microsoft Graphics Component、Microsoft Office、Microsoft Office SharePoint、Microsoft Scripting Engine、Microsoft Windows、Microsoft Windows DNS、Open Source Software、Servicing Stack Updates、SQL Server、Visual Studio、Windows Kernel、Windows Media、Windows RDP 以及 Windows Shell。

相关信息如下：

产品	CVE 编号	CVE 标题	严重程度
.NET Framework	CVE-2019-1113	.NET Framework 远程代码执行漏洞	Critical
.NET Framework	CVE-2019-1006	WCF/WIF SAML Token Authentication Bypass Vulnerability	Important
.NET Framework	CVE-2019-1083	.NET 拒绝服务漏洞	Important
ASP.NET	CVE-2019-1075	ASP.NET Core 欺骗漏洞	Moderate
Azure	CVE-2019-0962	Azure Automation 特权提升漏洞	Important

Azure DevOps	CVE-2019-1072	Azure DevOps Server and Team Foundation Server 远程代码执行漏洞	Critical
Azure DevOps	CVE-2019-1076	Team Foundation Server Cross-site Scripting Vulnerability	Important
Internet Explorer	CVE-2019-1063	Internet Explorer 内存破坏漏洞	Critical
Microsoft Browsers	CVE-2019-1104	Microsoft Browser 内存破坏漏洞	Critical
Microsoft Exchange Server	CVE-2019-1136	Microsoft Exchange Server 特权提升漏洞	Important
Microsoft Exchange Server	CVE-2019-1137	Microsoft Exchange Server 欺骗漏洞	Important

Microsoft Exchange Server	ADV190021	Outlook on the web 跨站脚本漏洞	Important
Microsoft Graphics Component	CVE-2019-1093	DirectWrite 信息泄露漏洞	Important
Microsoft Graphics Component	CVE-2019-1094	Windows GDI 信息泄露漏洞	Important
Microsoft Graphics Component	CVE-2019-1095	Windows GDI 信息泄露漏洞	Important
Microsoft Graphics Component	CVE-2019-1096	Win32k 信息泄露漏洞	Important
Microsoft Graphics Component	CVE-2019-1097	DirectWrite 信息泄露漏洞	Important
Microsoft Graphics Component	CVE-2019-1098	Windows GDI 信息泄露漏洞	Important

Microsoft Graphics Component	CVE-2019-1100	Windows GDI 信息泄露漏洞	Important
Microsoft Graphics Component	CVE-2019-1101	Windows GDI 信息泄露漏洞	Important
Microsoft Graphics Component	CVE-2019-1102	GDI+ 远程代码执行漏洞	Critical
Microsoft Graphics Component	CVE-2019-1116	Windows GDI 信息泄露漏洞	Important
Microsoft Graphics Component	CVE-2019-1117	DirectWrite 远程代码执行漏洞	Important
Microsoft Graphics Component	CVE-2019-1118	DirectWrite 远程代码执行漏洞	Important
Microsoft Graphics Component	CVE-2019-1119	DirectWrite 远程代码执行漏洞	Important
Microsoft Graphics Component	CVE-2019-1120	DirectWrite 远程代码执行漏洞	Important

Microsoft Graphics Component	CVE-2019-1121	DirectWrite 远程代码执行漏洞	Important
Microsoft Graphics Component	CVE-2019-1122	DirectWrite 远程代码执行漏洞	Important
Microsoft Graphics Component	CVE-2019-1123	DirectWrite 远程代码执行漏洞	Important
Microsoft Graphics Component	CVE-2019-1124	DirectWrite 远程代码执行漏洞	Important
Microsoft Graphics Component	CVE-2019-1127	DirectWrite 远程代码执行漏洞	Important
Microsoft Graphics Component	CVE-2019-1128	DirectWrite 远程代码执行漏洞	Important
Microsoft Graphics Component	CVE-2019-0999	DirectX 特权提升漏洞	Important
Microsoft Office	CVE-2019-1109	Microsoft Office 欺骗漏洞	Important

Microsoft Office	CVE-2019-1110	Microsoft Excel 远程代码执行漏洞	Important
Microsoft Office	CVE-2019-1111	Microsoft Excel 远程代码执行漏洞	Important
Microsoft Office	CVE-2019-1112	Microsoft Excel 信息泄露漏洞	Important
Microsoft Office	CVE-2019-1084	Microsoft Exchange 信息泄露漏洞	Important
Microsoft Office SharePoint	CVE-2019-1134	Microsoft Office SharePoint XSS Vulnerability	Important
Microsoft Scripting Engine	CVE-2019-1056	Scripting Engine 内存破坏漏洞	Critical
Microsoft Scripting Engine	CVE-2019-1059	Scripting Engine 内存破坏漏洞	Critical

Microsoft Scripting Engine	CVE-2019-1062	Chakra Scripting Engine 内存破坏漏洞	Critical
Microsoft Scripting Engine	CVE-2019-1092	Chakra Scripting Engine 内存破坏漏洞	Critical
Microsoft Scripting Engine	CVE-2019-1103	Chakra Scripting Engine 内存破坏漏洞	Critical
Microsoft Scripting Engine	CVE-2019-1106	Chakra Scripting Engine 内存破坏漏洞	Critical
Microsoft Scripting Engine	CVE-2019-1107	Chakra Scripting Engine 内存破坏漏洞	Critical
Microsoft Scripting Engine	CVE-2019-1001	Scripting Engine 内存破坏漏洞	Critical

Microsoft Scripting Engine	CVE-2019-1004	Scripting Engine 内存破坏漏洞	Critical
Microsoft Windows	CVE-2019-0865	SymCrypt 拒绝服务漏洞	Important
Microsoft Windows	CVE-2019-0887	Remote Desktop Services 远程代码执行漏洞	Important
Microsoft Windows	CVE-2019-0966	Windows Hyper-V 拒绝服务漏洞	Important
Microsoft Windows	CVE-2019-0975	ADFS 安全功能绕过漏洞	Important
Microsoft Windows	CVE-2019-1126	ADFS 安全功能绕过漏洞	Important
Microsoft Windows	CVE-2019-0785	Windows DHCP Server 远程代码执行漏洞	Critical

Microsoft Windows	CVE-2019-0880	Microsoft splwow64 特权提升漏洞	Important
Microsoft Windows	CVE-2019-1037	Windows Error Reporting 特权提升漏洞	Important
Microsoft Windows	CVE-2019-1067	Windows Kernel 特权提升漏洞	Important
Microsoft Windows	CVE-2019-1074	Microsoft Windows 特权提升漏洞	Important
Microsoft Windows	CVE-2019-1082	Microsoft Windows 特权提升漏洞	Important
Microsoft Windows	CVE-2019-1091	Microsoft unistore.dll 信息泄露漏洞	Important

Microsoft Windows	CVE-2019-1129	Windows 特权提升漏洞	Important
Microsoft Windows	CVE-2019-1130	Windows 特权提升漏洞	Important
Microsoft Windows DNS	CVE-2019-0811	Windows DNS Server 拒绝服务漏洞	Important
Microsoft Windows DNS	CVE-2019-1090	Windows dnsrlvr.dll 特权提升漏洞	Important
Open Source Software	CVE-2018-15664	Docker 特权提升漏洞	Important
Servicing Stack Updates	ADV990001	Latest Servicing Stack Updates	Critical
SQL Server	CVE-2019-1068	Microsoft SQL Server 远程代码执行漏洞	Important

Visual Studio	CVE-2019-1077	Visual Studio 特权提升漏洞	Important
Visual Studio	CVE-2019-1079	Visual Studio 信息泄露漏洞	Important
Windows Kernel	CVE-2019-1071	Windows Kernel 信息泄露漏洞	Important
Windows Kernel	CVE-2019-1073	Windows Kernel 信息泄露漏洞	Important
Windows Kernel	CVE-2019-1089	Windows RPCSS 特权提升漏洞	Important
Windows Kernel	CVE-2019-1132	Win32k 特权提升漏洞	Important
Windows Media	CVE-2019-1085	Windows WLAN Service 特权提升漏洞	Important

Windows Media	CVE-2019-1086	Windows Audio Service 特权提升漏洞	Important
Windows Media	CVE-2019-1087	Windows Audio Service 特权提升漏洞	Important
Windows Media	CVE-2019-1088	Windows Audio Service 特权提升漏洞	Important
Windows RDP	CVE-2019-1108	Remote Desktop Protocol Client 信息泄露漏洞	Important
Windows Shell	CVE-2019-1099	Windows GDI 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

ADV190021 - Outlook on the web Cross-Site Scripting Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
ADV190021 MITRE NVD	**CVE Title:** Outlook on the web Cross-Site Scripting Vulnerability **Description:** A cross-site scripting vulnerability has been discovered that affects Outlook on the web (formerly known as Outlook Web App) on-premise deployments. To exploit this vulnerability, an attacker must send a victim an email containing custom HTML content. The victim must then drag and drop an image that was included in the email	Important	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	into a new browser tab. Alternatively, a victim could paste the URL of the image into a new browser tab. The vulnerability requires that the image be sent in SVG format. Microsoft is addressing this vulnerability by recommending that administrators for Outlook on the web block SVG images. See the Mitigations section for instructions. **FAQ:** None **Mitigations:** **Workarounds:** None **Revision:** 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

ADV190021						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Exchange Server 2013		Important	Spoofing		Base: N/A Temporal: N/A Vector: N/A	
Microsoft Exchange Server 2010 Service Pack 3		Important	Spoofing		Base: N/A Temporal: N/A Vector: N/A	
Microsoft Exchange Server 2016		Important	Spoofing		Base: N/A Temporal: N/A Vector: N/A	
Microsoft Exchange Server 2019		Important	Spoofing		Base: N/A Temporal: N/A Vector: N/A	

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. **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:	Critical	Defense in Depth

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Product **SSU Package** **Date Released** Windows Server 2008 4493730 April 2019 Windows 7/Server 2008 R2 4490628 March 2019 Windows Server 2012 4504418 July 2019 Windows 8.1/Server 2012 R2 4504418 July 2019 Windows 10 4509090 July 2019 Windows 10 Version 1607/Server 2016 4509091 July 2019 Windows 10 Version 1703 4509092 July 2019 Windows 10 1709/Windows Server, version 1709 4509093 July 2019 Windows 10 1803/Windows Server, version 1803 4509094 July 2019 Windows 10 1809/Server 2019 4509095 July 2019 Windows 10 1903/Windows Server, version 1903 4509096 July 2019 **Mitigations:** None **Workarounds:** None		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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. 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. 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. 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. 1.2 12/03/2018 08:00:00		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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. 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. 5.0 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 Installation); Windows 10 Version 1803, and Windows Server, version 1803 (Server Core Installation). 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. 1.0 11/13/2018 08:00:00		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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. 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. 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. 3.1 12/11/2018 08:00:00 Updated supersedence information. This is an informational change only. 6.0 03/12/2019 07:00:00 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. 3.2 12/12/2018 08:00:00		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Fixed a typo in the FAQ. 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. 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.		

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**

ADV990001						
Windows 7 for 32-bit Systems Service Pack 1	4490628 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	4490628 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)	4490628 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	4490628 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	4490628 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)	4493730 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal:	Yes

ADV990001						
					N/A Vector: N/A	
Windows Server 2012	4504418 Servicing Stack Update	Critical	Defense in Depth	3173426	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2012 (Server Core installation)	4504418 Servicing Stack Update	Critical	Defense in Depth	3173426	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 8.1 for 32-bit systems	4504418 Servicing Stack Update	Critical	Defense in Depth	3173424	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 8.1 for x64-based systems	4504418 Servicing Stack Update	Critical	Defense in Depth	3173424	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2012 R2	4504418 Servicing Stack Update	Critical	Defense in Depth	3173424	Base: N/A Temporal: N/A Vector: N/A	Yes

ADV990001						
Windows Server 2012 R2 (Server Core installation)	4504418 Servicing Stack Update	Critical	Defense in Depth	3173424	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 for 32-bit Systems	4509090 Servicing Stack Update	Critical	Defense in Depth	4498353	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 for x64-based Systems	4509090 Servicing Stack Update	Critical	Defense in Depth	4498353	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2016	4509091 Servicing Stack Update	Critical	Defense in Depth	4503537	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1607 for 32-bit Systems	4509091 Servicing Stack Update	Critical	Defense in Depth	4503537	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1607 for x64-based Systems	4509091 Servicing Stack Update	Critical	Defense in Depth	4503537	Base: N/A Temporal:	Yes

ADV990001						
					N/A Vector: N/A	
Windows Server 2016 (Server Core installation)	4509091 Servicing Stack Update	Critical	Defense in Depth	4503537	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1703 for 32-bit Systems	4509092 Servicing Stack Update	Critical	Defense in Depth	4500640	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1703 for x64-based Systems	4509092 Servicing Stack Update	Critical	Defense in Depth	4500640	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1709 for 32-bit Systems	4509093 Servicing Stack Update	Critical	Defense in Depth	4500641	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1709 for x64-based Systems	4509093 Servicing Stack Update	Critical	Defense in Depth	4500641	Base: N/A Temporal: N/A Vector: N/A	Yes

ADV990001						
Windows 10 Version 1803 for 32-bit Systems	4509094 Servicing Stack Update	Critical	Defense in Depth	4497398	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1803 for x64-based Systems	4509094 Servicing Stack Update	Critical	Defense in Depth	4497398	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server, version 1803 (Server Core Installation)	4509094 Servicing Stack Update	Critical	Defense in Depth	4497398	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1803 for ARM64-based Systems	4509094 Servicing Stack Update	Critical	Defense in Depth	4497398	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1809 for 32-bit Systems	4509095 Servicing Stack Update	Critical	Defense in Depth	4504369	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1809 for x64-based Systems	4509095 Servicing Stack Update	Critical	Defense in Depth	4504369	Base: N/A Temporal:	Yes

ADV990001						
					N/A Vector: N/A	
Windows 10 Version 1809 for ARM64-based Systems	4509095 Servicing Stack Update	Critical	Defense in Depth	4504369	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2019	4509095 Servicing Stack Update	Critical	Defense in Depth	4504369	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2019 (Server Core installation)	4509095 Servicing Stack Update	Critical	Defense in Depth	4504369	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1709 for ARM64-based Systems	4509093 Servicing Stack Update	Critical	Defense in Depth	4500641	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1903 for 32-bit Systems	4509096 Servicing Stack Update	Critical	Defense in Depth	4498523	Base: N/A Temporal: N/A Vector: N/A	Yes

ADV990001						
Windows 10 Version 1903 for x64-based Systems	4509096 Servicing Stack Update	Critical	Defense in Depth	4498523	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1903 for ARM64-based Systems	4509096 Servicing Stack Update	Critical	Defense in Depth	4498523	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server, version 1903 (Server Core installation)	4509096 Servicing Stack Update	Critical	Defense in Depth	4498523	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4493730 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4493730 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4493730 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal:	Yes

ADV990001						
					N/A Vector: N/A	
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4493730 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2018-15664 - Docker Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-15664 MITRE NVD	**CVE Title:** Docker Elevation of Privilege Vulnerability **Description:** **Summary** CVE-2018-15664 describes a vulnerability in the Docker runtime (and the underlying community project, Moby) wherein a malicious/compromised container can acquire full read/write access to the host operating system where that container is running. The vulnerability depends on the way that the Docker runtime handles symbolic links and is	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	most directly exploitable through the Docker copy API (â€˜docker cpâ€™ in the Docker CLI). **What is the risk for Azure Kubernetes Service (AKS) and Azure IoT Edge customers?** The risk for AKS and Azure IoT Edge customers is minimal as the following need to be true: • A container on the host must be compromised. • The attacker must have access to the host machine, as the docker API is not exposed by default from outside of the host. **When will the vulnerability be fixed?** There is a pull request in review to fix this vulnerability. After the fix is merged in the upstream Moby project, we will build and release a new Moby build for use with AKS. For Azure IoT Edge customers, we will make the fixed Moby packages available along with installation instructions. **What can customers do in the interim?** We recommend that customers refrain from allowing the use of the Docker copy command on their AKS clusters and Azure IoT Edge devices.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Note that this article will be updated as additional details become available. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2018-15664						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2018-15664						
Azure IoT Edge	Release Notes Security Update	Important	Elevation of Privilege		Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Azure Kubernetes Service		Important	Elevation of Privilege		Base: N/A Temporal: N/A Vector: N/A	

CVE-2019-0785 - Windows DHCP Server Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0785 MITRE NVD	**CVE Title:** Windows DHCP Server Remote Code Execution Vulnerability **Description:** A memory corruption vulnerability exists in the Windows Server DHCP service when an attacker sends specially crafted packets to a DHCP failover server. An attacker who	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	successfully exploited the vulnerability could either run arbitrary code on the DHCP failover server or cause the DHCP service to become nonresponsive. To exploit the vulnerability, an attacker could send a specially crafted packet to a DHCP server. However, the DHCP server must be set to failover mode for the attack to succeed. The security update addresses the vulnerability by correcting how DHCP failover servers handle network packets. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0785						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows Server 2012	4507462 Monthly Rollup 4507464 Security Only	Critical	Remote Code Execution	4503285	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4507462 Monthly Rollup 4507464 Security Only	Critical	Remote Code Execution	4503285	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4507448 Monthly Rollup 4507457	Critical	Remote Code Execution	4503276	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0785						
	Security Only					
Windows Server 2012 R2 (Server Core installation)	4507448 Monthly Rollup 4507457 Security Only	Critical	Remote Code Execution	4503276	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4507460 Security Update	Critical	Remote Code Execution	4503267	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4507460 Security Update	Critical	Remote Code Execution	4503267	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server	4507435 Security Update	Critical	Remote Code Execution	4503286	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0785						
Core Installation)						
Windows Server 2019	4507469 Security Update	Critical	Remote Code Execution	4503327	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4507469 Security Update	Critical	Remote Code Execution	4503327	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4507453 Security Update	Critical	Remote Code Execution	4503293	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0811 - Windows DNS Server Denial of Service Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0811 MITRE NVD	**CVE Title:** Windows DNS Server Denial of Service Vulnerability **Description:** A denial of service vulnerability exists in Windows DNS Server when it fails to properly handle DNS queries. An attacker who successfully exploited this vulnerability could cause the DNS Server service to become nonresponsive. To exploit the vulnerability, an unauthenticated attacker could send malicious DNS queries to an affected server, resulting in a denial of service. However, the DNS server must be configured to use DNS Analytical Logging for the attack to succeed. The update addresses the vulnerability by correcting how Windows DNS Server processes DNS queries. **FAQ:** None **Mitigations:** None **Workarounds:** None	Important	Denial of Service

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0811						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows Server 2012 R2	4507448 Monthly Rollup 4507457 Security Only	Important	Denial of Service	4503276	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-2019-0811						
Windows Server 2012 R2 (Server Core installation)	4507448 Monthly Rollup 4507457 Security Only	Important	Denial of Service	4503276	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	4507460 Security Update	Important	Denial of Service	4503267	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)	4507460 Security Update	Important	Denial of Service	4503267	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)	4507435 Security Update	Important	Denial of Service	4503286	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	4507469 Security Update	Important	Denial of Service	4503327	Base: 7.5 Temporal: 6.7	Yes

CVE-2019-0811						
					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 2019 (Server Core installation)	4507469 Security Update	Important	Denial of Service	4503327	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)	4507453 Security Update	Important	Denial of Service	4503293	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-2019-0865 - SymCrypt Denial of Service Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0865 MITRE NVD	**CVE Title:** SymCrypt Denial of Service Vulnerability **Description:** A denial of service vulnerability exists when SymCrypt improperly handles a specially crafted digital signature.	Important	Denial of Service

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	An attacker could exploit the vulnerability by creating a specially crafted connection or message. The security update addresses the vulnerability by correcting the way SymCrypt handles digital signatures. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0865						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1703 for 32-bit Systems	4507450 Security Update	Important	Denial of Service	4503279	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	4507450 Security Update	Important	Denial of Service	4503279	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	4507455 Security Update	Important	Denial of Service	4503284	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	4507455 Security Update	Important	Denial of Service	4503284	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	4507435 Security Update	Important	Denial of Service	4503286	Base: 7.5 Temporal: 6.7	Yes

CVE-2019-0865						
1803 for 32-bit Systems					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 1803 for x64-based Systems	4507435 Security Update	Important	Denial of Service	4503286	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)	4507435 Security Update	Important	Denial of Service	4503286	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	4507435 Security Update	Important	Denial of Service	4503286	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	4507469 Security Update	Important	Denial of Service	4503327	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-2019-0865						
Windows 10 Version 1809 for x64-based Systems	4507469 Security Update	Important	Denial of Service	4503327	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 ARM64-based Systems	4507469 Security Update	Important	Denial of Service	4503327	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	4507469 Security Update	Important	Denial of Service	4503327	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)	4507469 Security Update	Important	Denial of Service	4503327	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-	4507455 Security Update	Important	Denial of Service	4503284	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-2019-0865						
based Systems						
Windows 10 Version 1903 for 32-bit Systems	4507453 Security Update	Important	Denial of Service	4503293	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	4507453 Security Update	Important	Denial of Service	4503293	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	4507453 Security Update	Important	Denial of Service	4503293	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)	4507453 Security Update	Important	Denial of Service	4503293	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-2019-0880 - Microsoft splwow64 Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0880 MITRE NVD	**CVE Title:** Microsoft splwow64 Elevation of Privilege Vulnerability **Description:** A local elevation of privilege vulnerability exists in how splwow64.exe handles certain calls. An attacker who successfully exploited the vulnerability could elevate privileges on an affected system from low-integrity to medium-integrity. This vulnerability by itself 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 (such as a remote code execution vulnerability or another elevation of privilege vulnerability) that is capable of leveraging the elevated privileges when code execution is attempted. **FAQ:** None **Mitigations:** None	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Workarounds: None **Revision:** 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0880						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows Server 2012	4507462 Monthly Rollup 4507464 Security Only	Important	Elevation of Privilege	4503285	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-2019-0880						
Windows Server 2012 (Server Core installation)	4507462 Monthly Rollup 4507464 Security Only	Important	Elevation of Privilege	4503285	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	4507448 Monthly Rollup 4507457 Security Only	Important	Elevation of Privilege	4503276	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	4507448 Monthly Rollup 4507457 Security Only	Important	Elevation of Privilege	4503276	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	4507448 Monthly Rollup 4507457 Security	Important	Elevation of Privilege	4503276	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-2019-0880						
	Only					
Windows RT 8.1	4507448 Monthly Rollup	Important	Elevation of Privilege	4503276	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)	4507448 Monthly Rollup 4507457 Security Only	Important	Elevation of Privilege	4503276	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	4507458 Security Update	Important	Elevation of Privilege	4503291	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 x64-based Systems	4507458 Security Update	Important	Elevation of Privilege	4503291	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	4507460 Security Update	Important	Elevation of Privilege	4503267	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-2019-0880						
Windows 10 Version 1607 for 32-bit Systems	4507460 Security Update	Important	Elevation of Privilege	4503267	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	4507460 Security Update	Important	Elevation of Privilege	4503267	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)	4507460 Security Update	Important	Elevation of Privilege	4503267	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 32-bit Systems	4507450 Security Update	Important	Elevation of Privilege	4503279	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	4507450 Security Update	Important	Elevation of Privilege	4503279	Base: 7 Temporal: 6.3	Yes

CVE-2019-0880						
x64-based Systems					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 32-bit Systems	4507455 Security Update	Important	Elevation of Privilege	4503284	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	4507455 Security Update	Important	Elevation of Privilege	4503284	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 32-bit Systems	4507435 Security Update	Important	Elevation of Privilege	4503286	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	4507435 Security Update	Important	Elevation of Privilege	4503286	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-2019-0880						
Windows Server, version 1803 (Server Core Installation)	4507435 Security Update	Important	Elevation of Privilege	4503286	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	4507435 Security Update	Important	Elevation of Privilege	4503286	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	4507469 Security Update	Important	Elevation of Privilege	4503327	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	4507469 Security Update	Important	Elevation of Privilege	4503327	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-2019-0880						
Windows 10 Version 1809 for ARM64-based Systems	4507469 Security Update	Important	Elevation of Privilege	4503327	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	4507469 Security Update	Important	Elevation of Privilege	4503327	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)	4507469 Security Update	Important	Elevation of Privilege	4503327	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 ARM64-based Systems	4507455 Security Update	Important	Elevation of Privilege	4503284	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-2019-0880						
Windows 10 Version 1903 for 32-bit Systems	4507453 Security Update	Important	Elevation of Privilege	4503293	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	4507453 Security Update	Important	Elevation of Privilege	4503293	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	4507453 Security Update	Important	Elevation of Privilege	4503293	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)	4507453 Security Update	Important	Elevation of Privilege	4503293	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-2019-0887 - Remote Desktop ServicesÂ Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0887 MITRE NVD	**CVE Title:** Remote Desktop ServicesÂ Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in Remote Desktop Services â€“ formerly known as Terminal Services â€“ when an authenticated attacker abuses clipboard redirection. An attacker who successfully exploited this vulnerability could execute arbitrary code on the victim system. 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 must already have compromised a system running Remote Desktop Services, and then wait for a victim system to connect to Remote Desktop Services. The update addresses the vulnerability by correcting how Remote Desktop Services handles clipboard redirection. **FAQ:**	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0887						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems	4507449 Monthly Rollup	Important	Remote Code Execution	4503292	Base: 8 Temporal: 7.2	Yes

CVE-2019-0887						
Service Pack 1	4507456 Security Only				Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 7 for x64-based Systems Service Pack 1	4507449 Monthly Rollup 4507456 Security Only	Important	Remote Code Execution	4503292	Base: 8 Temporal: 7.2 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/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)	4507449 Monthly Rollup 4507456 Security Only	Important	Remote Code Execution	4503292	Base: 8 Temporal: 7.2 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-	4507449 Monthly Rollup 4507456	Important	Remote Code Execution	4503292	Base: 8 Temporal: 7.2 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0887						
Based Systems Service Pack 1	Security Only					
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4507449 Monthly Rollup 4507456 Security Only	Important	Remote Code Execution	4503292	Base: 8 Temporal: 7.2 Vector: CVSS:3.0/AV:N/AC:L/PR:L/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)	4507452 Monthly Rollup 4507461 Security Only	Important	Remote Code Execution	4503273	Base: 8 Temporal: 7.2 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012	4507462 Monthly Rollup	Important	Remote Code Execution	4503285	Base: 8 Temporal: 7.2	Yes

CVE-2019-0887						
	4507464 Security Only				Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2012 (Server Core installation)	4507462 Monthly Rollup 4507464 Security Only	Important	Remote Code Execution	4503285	Base: 8 Temporal: 7.2 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4507448 Monthly Rollup 4507457 Security Only	Important	Remote Code Execution	4503276	Base: 8 Temporal: 7.2 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4507448 Monthly Rollup 4507457 Security Only	Important	Remote Code Execution	4503276	Base: 8 Temporal: 7.2 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0887						
Windows Server 2012 R2	4507448 Monthly Rollup 4507457 Security Only	Important	Remote Code Execution	4503276	Base: 8 Temporal: 7.2 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4507448 Monthly Rollup	Important	Remote Code Execution	4503276	Base: 8 Temporal: 7.2 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4507448 Monthly Rollup 4507457 Security Only	Important	Remote Code Execution	4503276	Base: 8 Temporal: 7.2 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4507458 Security Update	Important	Remote Code Execution	4503291	Base: 8 Temporal: 7.2 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-	4507458 Security Update	Important	Remote Code Execution	4503291	Base: 8 Temporal: 7.2	Yes

CVE-2019-0887						
based Systems					Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2016	4507460 Security Update	Important	Remote Code Execution	4503267	Base: 8 Temporal: 7.2 Vector: CVSS:3.0/AV:N/AC:L/PR:L/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	4507460 Security Update	Important	Remote Code Execution	4503267	Base: 8 Temporal: 7.2 Vector: CVSS:3.0/AV:N/AC:L/PR:L/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	4507460 Security Update	Important	Remote Code Execution	4503267	Base: 8 Temporal: 7.2 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4507460 Security Update	Important	Remote Code Execution	4503267	Base: 8 Temporal: 7.2 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0887						
Windows 10 Version 1703 for 32-bit Systems	4507450 Security Update	Important	Remote Code Execution	4503279	Base: 8 Temporal: 7.2 Vector: CVSS:3.0/AV:N/AC:L/PR:L/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	4507450 Security Update	Important	Remote Code Execution	4503279	Base: 8 Temporal: 7.2 Vector: CVSS:3.0/AV:N/AC:L/PR:L/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	4507455 Security Update	Important	Remote Code Execution	4503284	Base: 8 Temporal: 7.2 Vector: CVSS:3.0/AV:N/AC:L/PR:L/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	4507455 Security Update	Important	Remote Code Execution	4503284	Base: 8 Temporal: 7.2 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for	4507435 Security Update	Important	Remote Code Execution	4503286	Base: 8 Temporal: 7.2	Yes

CVE-2019-0887						
32-bit Systems					Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1803 for x64-based Systems	4507435 Security Update	Important	Remote Code Execution	4503286	Base: 8 Temporal: 7.2 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4507435 Security Update	Important	Remote Code Execution	4503286	Base: 8 Temporal: 7.2 Vector: CVSS:3.0/AV:N/AC:L/PR:L/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	4507435 Security Update	Important	Remote Code Execution	4503286	Base: 8 Temporal: 7.2 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for	4507469 Security Update	Important	Remote Code Execution	4503327	Base: 8 Temporal: 7.2	Yes

CVE-2019-0887						
32-bit Systems					Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1809 for x64-based Systems	4507469 Security Update	Important	Remote Code Execution	4503327	Base: 8 Temporal: 7.2 Vector: CVSS:3.0/AV:N/AC:L/PR:L/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	4507469 Security Update	Important	Remote Code Execution	4503327	Base: 8 Temporal: 7.2 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4507469 Security Update	Important	Remote Code Execution	4503327	Base: 8 Temporal: 7.2 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4507469 Security Update	Important	Remote Code Execution	4503327	Base: 8 Temporal: 7.2 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0887						
Windows 10 Version 1709 for ARM64-based Systems	4507455 Security Update	Important	Remote Code Execution	4503284	Base: 8 Temporal: 7.2 Vector: CVSS:3.0/AV:N/AC:L/PR:L/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	4507453 Security Update	Important	Remote Code Execution	4503293	Base: 8 Temporal: 7.2 Vector: CVSS:3.0/AV:N/AC:L/PR:L/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	4507453 Security Update	Important	Remote Code Execution	4503293	Base: 8 Temporal: 7.2 Vector: CVSS:3.0/AV:N/AC:L/PR:L/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	4507453 Security Update	Important	Remote Code Execution	4503293	Base: 8 Temporal: 7.2 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0887						
Windows Server, version 1903 (Server Core installation)	4507453 Security Update	Important	Remote Code Execution	4503293	Base: 8 Temporal: 7.2 Vector: CVSS:3.0/AV:N/AC:L/PR:L/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	4507452 Monthly Rollup 4507461 Security Only	Important	Remote Code Execution	4503273	Base: 8 Temporal: 7.2 Vector: CVSS:3.0/AV:N/AC:L/PR:L/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	4507452 Monthly Rollup 4507461 Security Only	Important	Remote Code Execution	4503273	Base: 8 Temporal: 7.2 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-	4507452 Monthly Rollup	Important	Remote Code Execution	4503273	Base: 8 Temporal: 7.2	Yes

CVE-2019-0887						
based Systems Service Pack 2	4507461 Security Only				Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/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)	4507452 Monthly Rollup 4507461 Security Only	Important	Remote Code Execution	4503273	Base: 8 Temporal: 7.2 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0962 - Azure Automation Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0962 MITRE NVD	**CVE Title:** Azure Automation Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in Azure Automation â€œRunAs accountâ€ runbooks for users with contributor role. This vulnerability could potentially allow members of an organization to access Key Vault secrets through a runbook, even if these members would personally not have access to that Key Vault. To exploit this vulnerability, an attacker must be a member of an organization who can run runbooks, with only global admins/co-admins who can create the â€œrun asâ€ account. Microsoft is addressing the vulnerability by providing the following scripts for existing RunAsAutomation accounts that modify existing roles by excluding access to KeyVault within Azure Automation account. • https://www.powershellgallery.com/packages/Check-AutomationRunAsAccountRoleAssignments • https://www.powershellgallery.com/packages/Update-AutomationRunAsAccountRoleAssignments	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	• https://www.powershellgallery.com/packages/Extend-AutomationRunAsAccountRoleAssignmentToKeyVault **FAQ:** **1. What is Azure Automation?** Azure Automation is an Azure service which executes PowerShell and Python runbooks on behalf of a user. As part of the Azure Automation service, a â€œRunAs accountâ€ may be created. The â€œRunAs accountâ€ is a Service Principal â€“ an Azure Active Directory app which can execute actions on a userâ€™s behalf. Azure Automation can use RunAs accounts inside of Azure Automation runbooks to access Azure resources in a programmatic way. **2. What do I need to do to protect my service against this vulnerability?** Microsoft is providing scripts that help users to: • Restrict Automation RunAs accounts from accessing Key Vaults. • Selectively grant Automation RunAs accounts permissions for specific Key Vaults. These scripts can be further customized by users to their individual needs. **3. Where can I find these scripts?**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	• https://www.powershellgallery.com/packages/Update-AutomationRunAsAccountRoleAssignments • https://www.powershellgallery.com/packages/Extend-AutomationRunAsAccountRoleAssignmentToKeyVault For more information about limiting Run As account permissions, see Manage Azure Automation Run As accounts. **4. How do I know if I need to run the script for RunAs accounts?** Microsoft has provided a script to help users determine if they are affected: • Check permissions on RunAs accounts: https://www.powershellgallery.com/packages/Check-AutomationRunAsAccountRoleAssignments **Mitigations:** None **Workarounds:** None		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0962						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Azure Automation	More information None	Important	Elevation of Privilege		Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0966 - Windows Hyper-V Denial of Service Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0966 MITRE NVD	**CVE Title:** Windows Hyper-V Denial of Service Vulnerability **Description:** A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate input from a privileged user on a guest operating system. To exploit the vulnerability, an attacker who already has a privileged account on a guest operating system, running as a virtual machine, could run a specially crafted application that causes a host machine to crash. To exploit the vulnerability, an attacker who already has a privileged account on a guest operating system, running as a virtual machine, could run a specially crafted application. The security update addresses the vulnerability by resolving a number of conditions where Hyper-V would fail to prevent a guest operating system from sending malicious requests. **FAQ:** None **Mitigations:** None	Important	Denial of Service

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Workarounds: None **Revision:** 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0966						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows Server 2016	4507460 Security Update	Important	Denial of Service	4503267	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0966						
Windows 10 Version 1607 for x64-based Systems	4507460 Security Update	Important	Denial of Service	4503267	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4507460 Security Update	Important	Denial of Service	4503267	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4507450 Security Update	Important	Denial of Service	4503279	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4507455 Security Update	Important	Denial of Service	4503284	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-	4507435 Security Update	Important	Denial of Service	4503286	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0966						
based Systems						
Windows Server, version 1803 (Server Core Installation)	4507435 Security Update	Important	Denial of Service	4503286	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4507469 Security Update	Important	Denial of Service	4503327	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4507469 Security Update	Important	Denial of Service	4503327	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4507469 Security Update	Important	Denial of Service	4503327	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-	4507453 Security Update	Important	Denial of Service	4503293	Base: 6.8 Temporal: 6.1	Yes

CVE-2019-0966						
based Systems					Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	
Windows Server, version 1903 (Server Core installation)	4507453 Security Update	Important	Denial of Service	4503293	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0975 - ADFS Security Feature Bypass Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0975 MITRE NVD	**CVE Title:** ADFS Security Feature Bypass Vulnerability **Description:** A security feature bypass vulnerability exists when Active Directory Federation Services (ADFS) improperly updates its list of banned IP addresses. To exploit this vulnerability, an attacker would have to convince a victim ADFS administrator to update the list of banned IP addresses. This security update corrects how ADFS updates its list of banned IP addresses.	Important	Security Feature Bypass

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0975						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2019-0975						
Windows Server 2016	4507460 Security Update	Important	Security Feature Bypass	4503267	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4507460 Security Update	Important	Security Feature Bypass	4503267	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4507435 Security Update	Important	Security Feature Bypass	4503286	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2019	4507469 Security Update	Important	Security Feature Bypass	4503327	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4507469 Security Update	Important	Security Feature Bypass	4503327	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2019-0975						
Windows Server, version 1903 (Server Core installation)	4507453 Security Update	Important	Security Feature Bypass	4503293	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2019-0999 - DirectX Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0999 MITRE NVD	**CVE Title:** DirectX Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when DirectX improperly handles 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.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The update addresses the vulnerability by correcting how DirectX handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0999						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	4507458 Security Update	Important	Elevation of Privilege	4503291	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	4507458 Security Update	Important	Elevation of Privilege	4503291	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	4507460 Security Update	Important	Elevation of Privilege	4503267	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	4507460 Security Update	Important	Elevation of Privilege	4503267	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	4507460 Security Update	Important	Elevation of Privilege	4503267	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-2019-0999						
Windows Server 2016 (Server Core installation)	4507460 Security Update	Important	Elevation of Privilege	4503267	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	4507450 Security Update	Important	Elevation of Privilege	4503279	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	4507450 Security Update	Important	Elevation of Privilege	4503279	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	4507455 Security Update	Important	Elevation of Privilege	4503284	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	4507455 Security Update	Important	Elevation of Privilege	4503284	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-2019-0999						
Windows 10 Version 1803 for 32-bit Systems	4507435 Security Update	Important	Elevation of Privilege	4503286	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	4507435 Security Update	Important	Elevation of Privilege	4503286	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)	4507435 Security Update	Important	Elevation of Privilege	4503286	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	4507435 Security Update	Important	Elevation of Privilege	4503286	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-2019-0999						
Windows 10 Version 1709 for ARM64-based Systems	4507455 Security Update	Important	Elevation of Privilege	4503284	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-2019-1001 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1001 MITRE NVD	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way the scripting engine handles objects in memory in Microsoft browsers. 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	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 designed to exploit the vulnerability through a Microsoft browser 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 browser 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 **Mitigations:** None **Workarounds:** None **Revision:** 1.0 07/09/2019 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-2019-1001						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1	4507434 IE Cumulative 4507449 Monthly Rollup	Critical	Remote Code Execution	4503292	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-2019-1001						
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1	4507434 IE Cumulative 4507449 Monthly Rollup	Critical	Remote Code Execution	4503292	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 Service Pack 1	4507434 IE Cumulative 4507449 Monthly Rollup	Moderate	Remote Code Execution	4503292	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	4507434 IE Cumulative	Moderate	Remote Code	4503259	Base: 6.4 Temporal: 5.8 Vector:	Yes

CVE-2019-1001						
Windows Server 2012			Execution		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 8.1 for 32-bit systems	4507448 Monthly Rollup 4507434 IE Cumulative	Critical	Remote Code Execution	4503259	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	4507448 Monthly Rollup 4507434 IE Cumulative	Critical	Remote Code Execution	4503259	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	4507448 Monthly Rollup 4507434 IE Cumulative	Moderate	Remote Code Execution	4503259	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-2019-1001						
Internet Explorer 11 on Windows RT 8.1	4507448 Monthly Rollup	Critical	Remote Code Execution	4503276	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	4507458 Security Update	Critical	Remote Code Execution	4503291	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	4507458 Security Update	Critical	Remote Code Execution	4503291	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	4507460 Security Update	Moderate	Remote Code Execution	4503267	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-2019-1001						
Server 2016						
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems	4507460 Security Update	Critical	Remote Code Execution	4503267	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	4507460 Security Update	Critical	Remote Code Execution	4503267	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	4507450 Security Update	Critical	Remote Code Execution	4503279	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-2019-1001						
1703 for 32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems	4507450 Security Update	Critical	Remote Code Execution	4503279	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 32-bit Systems	4507455 Security Update	Critical	Remote Code Execution	4503284	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	4507455 Security Update	Critical	Remote Code Execution	4503284	Base: 7.5 Temporal: 6.7 Vector:	Yes

CVE-2019-1001						
10 Version 1709 for x64-based Systems					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 10 Version 1803 for 32-bit Systems	4507435 Security Update	Critical	Remote Code Execution	4503286	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	4507435 Security Update	Critical	Remote Code Execution	4503286	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	4507435 Security Update	Critical	Remote Code	4503286	Base: 7.5 Temporal: 6.7 Vector:	Yes

CVE-2019-1001						
Windows 10 Version 1803 for ARM64-based Systems			Execution		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 10 Version 1809 for 32-bit Systems	4507469 Security Update	Critical	Remote Code Execution	4503327	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	4507469 Security Update	Critical	Remote Code Execution	4503327	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-2019-1001						
Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems	4507469 Security Update	Critical	Remote Code Execution	4503327	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	4507469 Security Update	Moderate	Remote Code Execution	4503327	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-	4507455 Security Update	Critical	Remote Code Execution	4503284	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-2019-1001						
based Systems						
Internet Explorer 11 on Windows 10 Version 1903 for 32-bit Systems	4507453 Security Update	Critical	Remote Code Execution	4503293	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	4507453 Security Update	Critical	Remote Code Execution	4503293	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	4507453 Security Update	Critical	Remote Code Execution	4503293	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-2019-1001						
1903 for ARM64-based Systems						
Microsoft Edge on Windows 10 for 32-bit Systems	4507458 Security Update	Critical	Remote Code Execution	4503291	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 on Windows 10 for x64-based Systems	4507458 Security Update	Critical	Remote Code Execution	4503291	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 on Windows Server 2016	4507460 Security Update	Moderate	Remote Code Execution	4503267	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 on Windows	4507460 Security Update	Critical	Remote Code	4503267	Base: 4.2 Temporal: 3.8	Yes

CVE-2019-1001						
10 Version 1607 for 32-bit Systems			Execution		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 on Windows 10 Version 1607 for x64-based Systems	4507460 Security Update	Critical	Remote Code Execution	4503267	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 on Windows 10 Version 1703 for 32-bit Systems	4507450 Security Update	Critical	Remote Code Execution	4503279	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 on Windows 10 Version 1703 for	4507450 Security Update	Critical	Remote Code Execution	4503279	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-2019-1001						
x64-based Systems						
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4507455 Security Update	Critical	Remote Code Execution	4503284	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 on Windows 10 Version 1709 for x64-based Systems	4507455 Security Update	Critical	Remote Code Execution	4503284	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 on Windows 10 Version 1803 for 32-bit Systems	4507435 Security Update	Critical	Remote Code Execution	4503286	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-2019-1001						
Microsoft Edge on Windows 10 Version 1803 for x64-based Systems	4507435 Security Update	Critical	Remote Code Execution	4503286	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 on Windows 10 Version 1803 for ARM64-based Systems	4507435 Security Update	Critical	Remote Code Execution	4503286	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 on Windows 10 Version 1809 for 32-bit Systems	4507469 Security Update	Critical	Remote Code Execution	4503327	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-2019-1001						
Microsoft Edge on Windows 10 Version 1809 for x64-based Systems	4507469 Security Update	Critical	Remote Code Execution	4503327	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 on Windows 10 Version 1809 for ARM64-based Systems	4507469 Security Update	Critical	Remote Code Execution	4503327	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 on Windows Server 2019	4507469 Security Update	Moderate	Remote Code Execution	4503327	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 on Windows	4507455 Security Update	Critical	Remote Code	4503284	Base: 4.2 Temporal: 3.8	Yes

CVE-2019-1001						
10 Version 1709 for ARM64-based Systems			Execution		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 on Windows 10 Version 1903 for 32-bit Systems	4507453 Security Update	Critical	Remote Code Execution	4503293	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 on Windows 10 Version 1903 for x64-based Systems	4507453 Security Update	Critical	Remote Code Execution	4503293	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 on Windows 10 Version	4507453 Security Update	Critical	Remote Code Execution	4503293	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-2019-1001						
1903 for ARM64-based Systems						
ChakraCore	Release Notes Security Update	Critical	Remote Code Execution	4503293	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1004 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1004 MITRE NVD	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer. 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	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 **Mitigations:** None **Workarounds:** None		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1004						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems	4507434 IE Cumulative 4507452 Monthly Rollup	Moderate	Remote Code Execution	4503273	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-2019-1004						
Service Pack 2						
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2	4507434 IE Cumulative 4507452 Monthly Rollup	Moderate	Remote Code Execution	4503273	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	4507434 IE Cumulative 4507449 Monthly Rollup	Critical	Remote Code Execution	4503292	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-2019-1004						
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1	4507434 IE Cumulative 4507449 Monthly Rollup	Critical	Remote Code Execution	4503292	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 Service Pack 1	4507434 IE Cumulative 4507449 Monthly Rollup	Moderate	Remote Code Execution	4503292	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-2019-1004						
Internet Explorer 11 on Windows Server 2012	4507434 IE Cumulative	Moderate	Remote Code Execution	4503259	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	4507448 Monthly Rollup 4507434 IE Cumulative	Critical	Remote Code Execution	4503259	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	4507448 Monthly Rollup 4507434 IE Cumulative	Critical	Remote Code Execution	4503259	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-2019-1004						
Internet Explorer 11 on Windows Server 2012 R2	4507448 Monthly Rollup 4507434 IE Cumulative	Moderate	Remote Code Execution	4503259	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	4507448 Monthly Rollup	Critical	Remote Code Execution	4503276	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	4507458 Security Update	Critical	Remote Code Execution	4503291	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	4507458 Security Update	Critical	Remote Code Execution	4503291	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-2019-1004						
x64-based Systems						
Internet Explorer 11 on Windows Server 2016	4507460 Security Update	Moderate	Remote Code Execution	4503267	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	4507460 Security Update	Critical	Remote Code Execution	4503267	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	4507460 Security Update	Critical	Remote Code Execution	4503267	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-2019-1004						
Version 1607 for x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems	4507450 Security Update	Critical	Remote Code Execution	4503279	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-	4507450 Security Update	Critical	Remote Code Execution	4503279	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-2019-1004						
based Systems						
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems	4507455 Security Update	Critical	Remote Code Execution	4503284	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	4507455 Security Update	Critical	Remote Code Execution	4503284	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-2019-1004						
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems	4507435 Security Update	Critical	Remote Code Execution	4503286	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	4507435 Security Update	Critical	Remote Code Execution	4503286	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	4507435 Security Update	Critical	Remote Code Execution	4503286	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-2019-1004						
10 Version 1803 for ARM64-based Systems						
Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems	4507469 Security Update	Critical	Remote Code Execution	4503327	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-	4507469 Security Update	Critical	Remote Code Execution	4503327	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-2019-1004						
based Systems						
Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems	4507469 Security Update	Critical	Remote Code Execution	4503327	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	4507469 Security Update	Moderate	Remote Code Execution	4503327	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	4507455 Security Update	Critical	Remote Code Execution	4503284	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-2019-1004						
Version 1709 for ARM64-based Systems						
Internet Explorer 11 on Windows 10 Version 1903 for 32-bit Systems	4507453 Security Update	Critical	Remote Code Execution	4503293	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-	4507453 Security Update	Critical	Remote Code Execution	4503293	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-2019-1004						
based Systems						
Internet Explorer 11 on Windows 10 Version 1903 for ARM64-based Systems	4507453 Security Update	Critical	Remote Code Execution	4503293	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	4507462 Monthly Rollup 4507434 IE Cumulative	Moderate	Remote Code Execution	4503259	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-2019-1006 - WCF/WIF SAML Token Authentication Bypass Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1006 MITRE NVD	**CVE Title:** WCF/WIF SAML Token Authentication Bypass Vulnerability **Description:** An authentication bypass vulnerability exists in Windows Communication Foundation (WCF) and Windows Identity Foundation (WIF), allowing signing of SAML tokens with arbitrary symmetric keys. This vulnerability allows an attacker to impersonate another user, which can lead to elevation of privileges. The vulnerability exists in WCF, WIF 3.5 and above in .NET Framework, WIF 1.0 component in Windows, WIF Nuget package, and WIF implementation in SharePoint. An unauthenticated attacker can exploit this by signing a SAML token with any arbitrary symmetric key. This security update addresses the issue by ensuring all versions of WCF and WIF validate the key used to sign SAML tokens correctly. **FAQ:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	What do I need to do to update SharePoint? Customers running affected versions of Microsoft SharePoint need to download and install both the applicable SharePoint update and the NuGet package for Microsoft.IdentityModel.dll to patch the vulnerability. See the Security Updates table for links to download the updates. **There are two updates for .NET Framework 3.5 installed on Windows 10 version 1809 and Windows Server 2019. How do I know which update I need to install?** The security updates for Windows 10 version 1809 and Windows Server 2019 include both .NET Framework 3.5 and 4.7.2 or 4.8. Customers running these versions of Windows 10 need to determine if they are also running .NET Framework 4.7.2 or .NET Framework 4.8. Install the security update that includes that second version of .NET Framework. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 07/09/2019 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-2019-1006						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4507449 Monthly Rollup 4507456 Security Only	Important	Elevation of Privilege	4503292	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 7 for x64-based Systems Service Pack 1	4507449 Monthly Rollup 4507456	Important	Elevation of Privilege	4503292	Base: N/A Temporal: N/A	Yes

CVE-2019-1006						
	Security Only				Vector: N/A	
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4507449 Monthly Rollup 4507456 Security Only	Important	Elevation of Privilege	4503292	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4507449 Monthly Rollup 4507456 Security Only	Important	Elevation of Privilege	4503292	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4507449 Monthly Rollup 4507456 Security Only	Important	Elevation of Privilege	4503292	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4507452 Monthly Rollup	Important	Elevation of Privilege	4503273	Base: N/A Temporal: N/A	Yes

CVE-2019-1006						
	4507461 Security Only				Vector: N/A	
Windows Server 2012	4507462 Monthly Rollup 4507464 Security Only	Important	Elevation of Privilege	4503285	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2012 (Server Core installation)	4507462 Monthly Rollup 4507464 Security Only	Important	Elevation of Privilege	4503285	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 8.1 for 32-bit systems	4507448 Monthly Rollup 4507457 Security Only	Important	Elevation of Privilege	4503276	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 8.1 for x64-based systems	4507448 Monthly	Important	Elevation of Privilege	4503276	Base: N/A Temporal:	Yes

CVE-2019-1006						
	Rollup 4507457 Security Only				N/A Vector: N/A	
Windows Server 2012 R2	4507448 Monthly Rollup 4507457 Security Only	Important	Elevation of Privilege	4503276	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows RT 8.1	4507448 Monthly Rollup	Important	Elevation of Privilege	4503276	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft SharePoint Foundation 2010 Service Pack 2	4475510 Security Update	Important	Elevation of Privilege	4464573	Base: N/A Temporal: N/A Vector: N/A	Maybe
Windows Server 2012 R2 (Server Core installation)	4507448 Monthly Rollup	Important	Elevation of Privilege	4503276	Base: N/A Temporal: N/A	Yes

CVE-2019-1006						
	4507457 Security Only				Vector: N/A	
Microsoft SharePoint Foundation 2013 Service Pack 1	4475527 Security Update	Important	Elevation of Privilege	4464602	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows 7 for 32-bit Systems Service Pack 1	4507420 Monthly Rollup 4507411 Security Only	Important	Elevation of Privilege	4503865	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows 7 for x64-based Systems Service Pack 1	4507420 Monthly Rollup 4507411 Security Only	Important	Elevation of Privilege	4503865	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4507420 Monthly Rollup	Important	Elevation of Privilege	4503865	Base: N/A Temporal: N/A	Maybe

CVE-2019-1006						
	4507411 Security Only				Vector: N/A	
Microsoft .NET Framework 4.5.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4507420 Monthly Rollup 4507411 Security Only	Important	Elevation of Privilege	4503865	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2012	4507412 Security Only 4507421 Monthly Rollup	Important	Elevation of Privilege	4499407; 4503866	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2012 (Server Core installation)	4507412 Security Only 4507421 Monthly Rollup	Important	Elevation of Privilege	4499407; 4503866	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows 8.1 for 32-bit systems	4507413 Security	Important	Elevation of Privilege	4499408; 4503867	Base: N/A Temporal:	Maybe

CVE-2019-1006						
	Only 4507422 Monthly Rollup				N/A Vector: N/A	
Microsoft .NET Framework 4.5.2 on Windows 8.1 for x64-based systems	4507413 Security Only 4507422 Monthly Rollup	Important	Elevation of Privilege	4499408; 4503867	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2012 R2	4507413 Security Only 4507422 Monthly Rollup	Important	Elevation of Privilege	4499408; 4503867	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows RT 8.1	4507422 Monthly Rollup	Important	Elevation of Privilege	4499408; 4503867	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2012 R2 (Server Core installation)	4507413 Security	Important	Elevation of Privilege	4499408; 4503867	Base: N/A Temporal:	Maybe

CVE-2019-1006						
	Only 4507422 Monthly Rollup				N/A Vector: N/A	
Microsoft .NET Framework 4.5.2 on Windows Server 2008 for 32-bit Systems Service Pack 2	4507423 Monthly Rollup 4507414 Security Only	Important	Elevation of Privilege	4489489; 4499409	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2008 for x64-based Systems Service Pack 2	4507423 Monthly Rollup 4507414 Security Only	Important	Elevation of Privilege	4489489; 4499409	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6 on Windows Server 2008 for 32-bit Systems Service Pack 2	4507423 Monthly Rollup 4507414 Security Only	Important	Elevation of Privilege	4489489; 4499409	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1006						
Microsoft .NET Framework 4.6 on Windows Server 2008 for x64-based Systems Service Pack 2	4507423 Monthly Rollup 4507414 Security Only	Important	Elevation of Privilege	4489489; 4499409	Base: N/A Temporal: N/A Vector: N/A	Maybe
Windows 10 for 32-bit Systems	4507458 Security Update	Important	Elevation of Privilege	4503291	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 for x64-based Systems	4507458 Security Update	Important	Elevation of Privilege	4503291	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2016	4507460 Security Update	Important	Elevation of Privilege	4503267	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1607 for 32-bit Systems	4507460 Security	Important	Elevation of Privilege	4503267	Base: N/A Temporal:	Yes

CVE-2019-1006						
	Update				N/A Vector: N/A	
Windows 10 Version 1607 for x64-based Systems	4507460 Security Update	Important	Elevation of Privilege	4503267	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2016 (Server Core installation)	4507460 Security Update	Important	Elevation of Privilege	4503267	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft SharePoint Enterprise Server 2016	4475520 Security Update	Important	Elevation of Privilege	4464594	Base: N/A Temporal: N/A Vector: N/A	Maybe
Windows 10 Version 1703 for 32-bit Systems	4507450 Security Update	Important	Elevation of Privilege	4503279	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-1006						
Windows 10 Version 1703 for x64-based Systems	4507450 Security Update	Important	Elevation of Privilege	4503279	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft SharePoint Enterprise Server 2013 Service Pack 1	4475522 Security Update	Important	Elevation of Privilege	4464597	Base: N/A Temporal: N/A Vector: N/A	Maybe
Windows 10 Version 1709 for 32-bit Systems	4507455 Security Update	Important	Elevation of Privilege	4503284	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1709 for x64-based Systems	4507455 Security Update	Important	Elevation of Privilege	4503284	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1803 for 32-bit Systems	4507435 Security Update	Important	Elevation of Privilege	4503286	Base: N/A Temporal: N/A	Yes

CVE-2019-1006						
					Vector: N/A	
Windows 10 Version 1803 for x64-based Systems	4507435 Security Update	Important	Elevation of Privilege	4503286	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server, version 1803 (Server Core Installation)	4507435 Security Update	Important	Elevation of Privilege	4503286	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.6/4.6.1/4.6.2 on Windows 10 for 32-bit Systems	4507458 Security Update	Important	Elevation of Privilege	4503291	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.6/4.6.1/4.6.2 on Windows 10 for x64-based Systems	4507458 Security Update	Important	Elevation of Privilege	4503291	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-1006						
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 7 for 32-bit Systems Service Pack 1	4507420 Monthly Rollup 4507411 Security Only	Important	Elevation of Privilege	4503291	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 7 for x64-based Systems Service Pack 1	4507420 Monthly Rollup 4507411 Security Only	Important	Elevation of Privilege	4503291	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4507420 Monthly Rollup 4507411 Security Only	Important	Elevation of Privilege	4503291	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4507420 Monthly Rollup 4507411 Security	Important	Elevation of Privilege	4503291	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1006						
	Only					
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012	4507421 Monthly Rollup 4507412 Security Only	Important	Elevation of Privilege	4499407; 4503866	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012 (Server Core installation)	4507421 Monthly Rollup 4507412 Security Only	Important	Elevation of Privilege	4499407; 4503866	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 8.1 for 32-bit systems	4507413 Security Only 4507422 Monthly Rollup	Important	Elevation of Privilege	4499408; 4503867	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 8.1 for x64-based systems	4507422 Monthly Rollup 4507413	Important	Elevation of Privilege	4499408; 4503867	Base: N/A Temporal: N/A	Maybe

CVE-2019-1006						
	Security Only				Vector: N/A	
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012 R2	4507422 Monthly Rollup 4507413 Security Only	Important	Elevation of Privilege	4499408; 4503867	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows RT 8.1	4507422 Monthly Rollup	Important	Elevation of Privilege	4499408; 4503867	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012 R2 (Server Core installation)	4507422 Monthly Rollup 4507413 Security Only	Important	Elevation of Privilege	4499408; 4503867	Base: N/A Temporal: N/A Vector: N/A	Maybe
Windows 10 Version 1803 for ARM64-based Systems	4507435 Security Update	Important	Elevation of Privilege	4503286	Base: N/A Temporal: N/A	Yes

CVE-2019-1006						
					Vector: N/A	
Windows 10 Version 1809 for 32-bit Systems	4507469 Security Update	Important	Elevation of Privilege	4503327	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1809 for x64-based Systems	4507469 Security Update	Important	Elevation of Privilege	4503327	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1809 for ARM64-based Systems	4507469 Security Update	Important	Elevation of Privilege	4503327	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2019	4507469 Security Update	Important	Elevation of Privilege	4503327	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-1006						
Windows Server 2019 (Server Core installation)	4507469 Security Update	Important	Elevation of Privilege	4503327	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1709 for ARM64-based Systems	4507455 Security Update	Important	Elevation of Privilege	4503284	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft SharePoint Server 2019	4475529 Security Update	Important	Elevation of Privilege	4475512	Base: N/A Temporal: N/A Vector: N/A	Maybe
Windows 10 Version 1903 for 32-bit Systems	4507453 Security Update	Important	Elevation of Privilege	4503293	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1903 for x64-based Systems	4507453 Security Update	Important	Elevation of Privilege	4503293	Base: N/A Temporal: N/A	Yes

CVE-2019-1006						
					Vector: N/A	
Windows 10 Version 1903 for ARM64-based Systems	4507453 Security Update	Important	Elevation of Privilege	4503293	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server, version 1903 (Server Core installation)	4507453 Security Update	Important	Elevation of Privilege	4503293	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.8 on Windows 7 for 32-bit Systems Service Pack 1	4507420 Monthly Rollup 4507411 Security Only	Important	Elevation of Privilege	4499406; 4503865	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 7 for x64-based Systems Service Pack 1	4507420 Monthly Rollup 4507411 Security	Important	Elevation of Privilege	4499406; 4503865	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1006						
	Only					
Microsoft .NET Framework 4.8 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4507420 Monthly Rollup 4507411 Security Only	Important	Elevation of Privilege	4499406; 4503865	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4507420 Monthly Rollup 4507411 Security Only	Important	Elevation of Privilege	4499406; 4503865	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2012	4507421 Monthly Rollup 4507412 Security Only	Important	Elevation of Privilege	4499407; 4503866	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2012 (Server Core installation)	4507421 Monthly Rollup 4507412	Important	Elevation of Privilege	4499407; 4503866	Base: N/A Temporal: N/A	Maybe

CVE-2019-1006						
	Security Only				Vector: N/A	
Microsoft .NET Framework 4.8 on Windows 8.1 for 32-bit systems	4507422 Monthly Rollup 4507413 Security Only	Important	Elevation of Privilege	4499408; 4503867	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 8.1 for x64-based systems	4507422 Monthly Rollup 4507413 Security Only	Important	Elevation of Privilege	4499408; 4503867	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2012 R2	4507422 Monthly Rollup 4507413 Security Only	Important	Elevation of Privilege	4499408; 4503867	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows RT 8.1	4507422 Monthly Rollup	Important	Elevation of Privilege	4499408; 4503867	Base: N/A Temporal: N/A	Maybe

CVE-2019-1006						
					Vector: N/A	
Microsoft .NET Framework 4.8 on Windows Server 2012 R2 (Server Core installation)	4507422 Monthly Rollup 4507413 Security Only	Important	Elevation of Privilege	4499408; 4503867	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2016	4506986 Security Update	Important	Elevation of Privilege	4495610; 4502560	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1607 for 32-bit Systems	4506986 Security Update	Important	Elevation of Privilege	4495610; 4502560	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1607 for x64-based Systems	4506986 Security Update	Important	Elevation of Privilege	4495610; 4502560	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1006						
Microsoft .NET Framework 4.8 on Windows Server 2016 (Server Core installation)	4506986 Security Update	Important	Elevation of Privilege	4495610; 4502560	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1703 for 32-bit Systems	4506987 Security Update	Important	Elevation of Privilege	4495611; 4502561	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1703 for x64-based Systems	4506986 Security Update	Important	Elevation of Privilege	4495610; 4502560	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1709 for 32-bit Systems	4506988 Security Update	Important	Elevation of Privilege	4495613; 4502562	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1709 for x64-based Systems	4506986 Security Update	Important	Elevation of Privilege	4495610; 4502560	Base: N/A Temporal: N/A	Maybe

CVE-2019-1006						
					Vector: N/A	
Microsoft .NET Framework 4.8 on Windows 10 Version 1803 for 32-bit Systems	4506989 Security Update	Important	Elevation of Privilege	4495616; 4502563	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1803 for x64-based Systems	4506989 Security Update	Important	Elevation of Privilege	4495616; 4502563	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server, version 1803 (Server Core Installation)	4506989 Security Update	Important	Elevation of Privilege	4495616; 4502563	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 1809 for 32-bit Systems	4507419 Security Update	Important	Elevation of Privilege	4486553; 4499405; 4503864	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1006						
Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 1809 for x64-based Systems	4507419 Security Update	Important	Elevation of Privilege	4486553; 4499405; 4503864	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 AND 4.8 on Windows Server 2019	4507419 Security Update	Important	Elevation of Privilege	4486553; 4499405; 4503864	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 AND 4.8 on Windows Server 2019 (Server Core installation)	4507419 Security Update	Important	Elevation of Privilege	4486553; 4499405; 4503864	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 1903 for 32-bit Systems	4506991 Security Update	Important	Elevation of Privilege	4495620; 4502584	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 1903 for x64-based Systems	4506991 Security Update	Important	Elevation of Privilege	4495620; 4502584	Base: N/A Temporal: N/A	Maybe

CVE-2019-1006						
					Vector: N/A	
Microsoft .NET Framework 3.5 AND 4.8 on Windows Server, version 1903 (Server Core installation)	4506991 Security Update	Important	Elevation of Privilege	4495620; 4502584	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 AND 4.7.2 on Windows 10 Version 1809 for 32-bit Systems	4507419 Security Update	Important	Elevation of Privilege	4486553; 4499405; 4503864	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 AND 4.7.2 on Windows 10 Version 1809 for x64-based Systems	4507419 Security Update	Important	Elevation of Privilege	4486553; 4499405; 4503864	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 AND 4.7.2 on Windows Server 2019	4507419 Security Update	Important	Elevation of Privilege	4486553; 4499405; 4503864	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1006						
Microsoft .NET Framework 3.5 AND 4.7.2 on Windows Server 2019 (Server Core installation)	4507419 Security Update	Important	Elevation of Privilege	4486553; 4499405; 4503864	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft.IdentityModel 7.0.0	Release Notes Security Update	Important	Elevation of Privilege	4486553; 4499405; 4503864	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2012	4507412 Security Only 4507421 Monthly Rollup	Important	Elevation of Privilege	4499407; 4503866	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2012 (Server Core installation)	4507412 Security Only 4507421 Monthly Rollup	Important	Elevation of Privilege	4499407; 4503866	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1006						
Microsoft .NET Framework 3.5 on Windows 8.1 for 32-bit systems	4507413 Security Only 4507422 Monthly Rollup	Important	Elevation of Privilege	4499408; 4503867	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows 8.1 for x64-based systems	4507413 Security Only 4507422 Monthly Rollup	Important	Elevation of Privilege	4499408; 4503867	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2012 R2	4507413 Security Only 4507422 Monthly Rollup	Important	Elevation of Privilege	4499408; 4503867	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2012 R2 (Server Core installation)	4507413 Security Only 4507422 Monthly	Important	Elevation of Privilege	4499408; 4503867	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1006						
	Rollup					
Microsoft .NET Framework 3.5 on Windows 10 for 32-bit Systems	4507458 Security Update	Important	Elevation of Privilege	4503291	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 for x64-based Systems	4507458 Security Update	Important	Elevation of Privilege	4503291	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows Server 2016	4507460 Security Update	Important	Elevation of Privilege	4503267	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1607 for 32-bit Systems	4507460 Security Update	Important	Elevation of Privilege	4503267	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1607 for x64-based Systems	4507460 Security	Important	Elevation of Privilege	4503267	Base: N/A Temporal:	Yes

CVE-2019-1006						
	Update				N/A Vector: N/A	
Microsoft .NET Framework 3.5 on Windows Server 2016 (Server Core installation)	4507460 Security Update	Important	Elevation of Privilege	4503267	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1703 for 32-bit Systems	4507450 Security Update	Important	Elevation of Privilege	4503279	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1703 for x64-based Systems	4507450 Security Update	Important	Elevation of Privilege	4503279	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1709 for 32-bit Systems	4507455 Security Update	Important	Elevation of Privilege	4503284	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-1006						
Microsoft .NET Framework 3.5 on Windows 10 Version 1709 for x64-based Systems	4507455 Security Update	Important	Elevation of Privilege	4503284	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1803 for 32-bit Systems	4507435 Security Update	Important	Elevation of Privilege	4503286	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1803 for x64-based Systems	4507435 Security Update	Important	Elevation of Privilege	4503286	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows Server, version 1803 (Server Core Installation)	4507435 Security Update	Important	Elevation of Privilege	4503286	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for Itanium-Based Systems Service Pack 2	4507414 Security Only	Important	Elevation of Privilege	4499409; 4503868	Base: N/A Temporal: N/A	Maybe

CVE-2019-1006						
	4507423 Monthly Rollup				Vector: N/A	
Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for 32-bit Systems Service Pack 2	4507414 Security Only 4507423 Monthly Rollup	Important	Elevation of Privilege	4499409; 4503868	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for x64-based Systems Service Pack 2	4507414 Security Only 4507423 Monthly Rollup	Important	Elevation of Privilege	4499409; 4503868	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 2.0 Service Pack 2 on Windows Server 2008 for Itanium-Based Systems Service Pack 2	4507414 Security Only 4507423 Monthly Rollup	Important	Elevation of Privilege	4499409; 4503868	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1006						
Microsoft .NET Framework 2.0 Service Pack 2 on Windows Server 2008 for 32-bit Systems Service Pack 2	4507414 Security Only 4507423 Monthly Rollup	Important	Elevation of Privilege	4499409; 4503868	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 2.0 Service Pack 2 on Windows Server 2008 for x64-based Systems Service Pack 2	4507414 Security Only 4507423 Monthly Rollup	Important	Elevation of Privilege	4499409; 4503868	Base: N/A Temporal: N/A Vector: N/A	Maybe
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4507452 Monthly Rollup 4507461 Security Only	Important	Elevation of Privilege	4503273	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4507452 Monthly Rollup 4507461 Security	Important	Elevation of Privilege	4503273	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-1006						
	Only					
Windows Server 2008 for x64-based Systems Service Pack 2	4507452 Monthly Rollup 4507461 Security Only	Important	Elevation of Privilege	4503273	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4507452 Monthly Rollup 4507461 Security Only	Important	Elevation of Privilege	4503273	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5.1 on Windows 7 for 32-bit Systems Service Pack 1	4507411 Security Only 4507420 Monthly Rollup	Important	Elevation of Privilege	4499406; 4503865	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5.1 on Windows 7 for x64-based Systems Service Pack 1	4507411 Security Only 4507420	Important	Elevation of Privilege	4499406; 4503865	Base: N/A Temporal: N/A	Maybe

CVE-2019-1006						
	Monthly Rollup				Vector: N/A	
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4507411 Security Only 4507420 Monthly Rollup	Important	Elevation of Privilege	4499406; 4503865	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4507411 Security Only 4507420 Monthly Rollup	Important	Elevation of Privilege	4499406; 4503865	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4507411 Security Only 4507420 Monthly Rollup	Important	Elevation of Privilege	4499406; 4503865	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1037 - Windows Error Reporting Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1037 MITRE NVD	**CVE Title:** Windows Error Reporting Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in the way Windows Error Reporting (WER) handles files. 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 administrator privileges. To exploit the vulnerability, an attacker must first gain unprivileged execution on a victim system. The security update addresses the vulnerability by correcting the way WER handles files. **FAQ:** None **Mitigations:** None	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Workarounds: None **Revision:** 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1037						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1709 for 32-bit Systems	4507455 Security Update	Important	Elevation of Privilege	4503284	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-2019-1037						
Windows 10 Version 1709 for x64-based Systems	4507455 Security Update	Important	Elevation of Privilege	4503284	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 32-bit Systems	4507435 Security Update	Important	Elevation of Privilege	4503286	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	4507435 Security Update	Important	Elevation of Privilege	4503286	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)	4507435 Security Update	Important	Elevation of Privilege	4503286	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-2019-1037						
Windows 10 Version 1803 for ARM64-based Systems	4507435 Security Update	Important	Elevation of Privilege	4503286	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	4507469 Security Update	Important	Elevation of Privilege	4503327	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	4507469 Security Update	Important	Elevation of Privilege	4503327	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	4507469 Security Update	Important	Elevation of Privilege	4503327	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-2019-1037						
Windows Server 2019	4507469 Security Update	Important	Elevation of Privilege	4503327	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)	4507469 Security Update	Important	Elevation of Privilege	4503327	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 ARM64-based Systems	4507455 Security Update	Important	Elevation of Privilege	4503284	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	4507453 Security Update	Important	Elevation of Privilege	4503293	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	4507453 Security Update	Important	Elevation of Privilege	4503293	Base: 7 Temporal: 6.3	Yes

CVE-2019-1037						
x64-based Systems					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	4507453 Security Update	Important	Elevation of Privilege	4503293	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)	4507435 Security Update	Important	Elevation of Privilege	4503286	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-2019-1056 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1056 MITRE NVD	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer. 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 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1056						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1	4507434 IE Cumulative 4507449 Monthly Rollup	Critical	Remote Code Execution	4503292	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 7 for x64-based Systems Service Pack 1	4507434 IE Cumulative 4507449 Monthly Rollup	Critical	Remote Code Execution	4503292	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-2019-1056						
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4507434 IE Cumulative 4507449 Monthly Rollup	Moderate	Remote Code Execution	4503292	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 Server 2012	4507434 IE Cumulative	Moderate	Remote Code Execution	4503259	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	4507448 Monthly Rollup 4507434 IE Cumulative	Critical	Remote Code Execution	4503259	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-2019-1056						
32-bit systems						
Internet Explorer 11 on Windows 8.1 for x64-based systems	4507448 Monthly Rollup 4507434 IE Cumulative	Critical	Remote Code Execution	4503259	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	4507448 Monthly Rollup 4507434 IE Cumulative	Moderate	Remote Code Execution	4503259	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	4507448 Monthly Rollup	Critical	Remote Code Execution	4503276	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-2019-1056						
Internet Explorer 11 on Windows 10 for 32-bit Systems	4507458 Security Update	Critical	Remote Code Execution	4503291	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	4507458 Security Update	Critical	Remote Code Execution	4503291	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 2016	4507460 Security Update	Moderate	Remote Code Execution	4503267	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-2019-1056						
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems	4507460 Security Update	Critical	Remote Code Execution	4503267	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	4507460 Security Update	Critical	Remote Code Execution	4503267	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	4507450 Security Update	Critical	Remote Code Execution	4503279	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-2019-1056						
10 Version 1703 for 32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems	4507450 Security Update	Critical	Remote Code Execution	4503279	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	4507455 Security Update	Critical	Remote Code Execution	4503284	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-2019-1056						
32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems	4507455 Security Update	Critical	Remote Code Execution	4503284	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 32-bit Systems	4507435 Security Update	Critical	Remote Code Execution	4503286	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-2019-1056						
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems	4507435 Security Update	Critical	Remote Code Execution	4503286	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	4507435 Security Update	Critical	Remote Code Execution	4503286	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	4507469 Security Update	Critical	Remote Code Execution	4503327	Base: 7.5 Temporal: 6.7	Yes

CVE-2019-1056						
Windows 10 Version 1809 for 32-bit Systems					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 10 Version 1809 for x64-based Systems	4507469 Security Update	Critical	Remote Code Execution	4503327	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	4507469 Security Update	Critical	Remote Code Execution	4503327	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-2019-1056						
ARM64-based Systems						
Internet Explorer 11 on Windows Server 2019	4507469 Security Update	Moderate	Remote Code Execution	4503327	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	4507455 Security Update	Critical	Remote Code Execution	4503284	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	4507453 Security Update	Critical	Remote Code Execution	4503293	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-2019-1056						
10 Version 1903 for 32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1903 for x64-based Systems	4507453 Security Update	Critical	Remote Code Execution	4503293	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 ARM64-	4507453 Security Update	Critical	Remote Code Execution	4503293	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-2019-1056						
based Systems						

CVE-2019-1059 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1059 MITRE NVD	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer. 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	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 **Mitigations:** None **Workarounds:** None **Revision:** 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1059						
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	4507434 IE Cumulative 4507452 Monthly Rollup	Moderate	Remote Code Execution	4503273	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 9 on Windows Server 2008 for	4507434 IE Cumulative 4507452 Monthly Rollup	Moderate	Remote Code Execution	4503273	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-2019-1059						
x64-based Systems Service Pack 2						
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1	4507434 IE Cumulative 4507449 Monthly Rollup	Critical	Remote Code Execution	4503292	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 7 for x64-based Systems	4507434 IE Cumulative 4507449 Monthly Rollup	Critical	Remote Code Execution	4503292	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-2019-1059						
Service Pack 1						
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4507434 IE Cumulative 4507449 Monthly Rollup	Moderate	Remote Code Execution	4503292	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 Server 2012	4507434 IE Cumulative	Moderate	Remote Code Execution	4503259	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	4507448 Monthly Rollup 4507434 IE	Critical	Remote Code Execution	4503259	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-2019-1059						
8.1 for 32-bit systems	Cumulative					
Internet Explorer 11 on Windows 8.1 for x64-based systems	4507448 Monthly Rollup 4507434 IE Cumulative	Critical	Remote Code Execution	4503259	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	4507448 Monthly Rollup 4507434 IE Cumulative	Moderate	Remote Code Execution	4503259	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	4507448 Monthly Rollup	Critical	Remote Code Execution	4503276	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-2019-1059						
Internet Explorer 11 on Windows 10 for 32-bit Systems	4507458 Security Update	Critical	Remote Code Execution	4503291	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	4507458 Security Update	Critical	Remote Code Execution	4503291	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 2016	4507460 Security Update	Moderate	Remote Code Execution	4503267	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-2019-1059						
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems	4507460 Security Update	Critical	Remote Code Execution	4503267	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	4507460 Security Update	Critical	Remote Code Execution	4503267	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	4507450 Security Update	Critical	Remote Code Execution	4503279	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-2019-1059						
10 Version 1703 for 32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems	4507450 Security Update	Critical	Remote Code Execution	4503279	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	4507455 Security Update	Critical	Remote Code Execution	4503284	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-2019-1059						
32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems	4507455 Security Update	Critical	Remote Code Execution	4503284	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 32-bit Systems	4507435 Security Update	Critical	Remote Code Execution	4503286	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-2019-1059						
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems	4507435 Security Update	Critical	Remote Code Execution	4503286	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	4507435 Security Update	Critical	Remote Code Execution	4503286	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	4507469 Security Update	Critical	Remote Code Execution	4503327	Base: 7.5 Temporal: 6.7	Yes

CVE-2019-1059						
Windows 10 Version 1809 for 32-bit Systems					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 10 Version 1809 for x64-based Systems	4507469 Security Update	Critical	Remote Code Execution	4503327	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	4507469 Security Update	Critical	Remote Code Execution	4503327	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-2019-1059						
ARM64-based Systems						
Internet Explorer 11 on Windows Server 2019	4507469 Security Update	Moderate	Remote Code Execution	4503327	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	4507455 Security Update	Critical	Remote Code Execution	4503284	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	4507453 Security Update	Critical	Remote Code Execution	4503293	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-2019-1059						
10 Version 1903 for 32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1903 for x64-based Systems	4507453 Security Update	Critical	Remote Code Execution	4503293	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 ARM64-	4507453 Security Update	Critical	Remote Code Execution	4503293	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-2019-1059						
based Systems						
Internet Explorer 10 on Windows Server 2012	4507462 Monthly Rollup 4507434 IE Cumulative	Moderate	Remote Code Execution	4503259	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-2019-1062 - Chakra Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1062 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	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 **Workarounds:** None		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1062						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4507458 Security Update	Critical	Remote Code Execution	4503291	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 on Windows	4507458 Security Update	Critical	Remote Code Execution	4503291	Base: 4.2 Temporal: 3.8	Yes

CVE-2019-1062						
10 for x64-based Systems					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 on Windows Server 2016	4507460 Security Update	Moderate	Remote Code Execution	4503267	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 on Windows 10 Version 1607 for 32-bit Systems	4507460 Security Update	Critical	Remote Code Execution	4503267	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 on Windows 10 Version 1607 for x64-based Systems	4507460 Security Update	Critical	Remote Code Execution	4503267	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-2019-1062						
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4507450 Security Update	Critical	Remote Code Execution	4503279	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 on Windows 10 Version 1703 for x64-based Systems	4507450 Security Update	Critical	Remote Code Execution	4503279	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 on Windows 10 Version 1709 for 32-bit Systems	4507455 Security Update	Critical	Remote Code Execution	4503284	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-2019-1062						
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4507455 Security Update	Critical	Remote Code Execution	4503284	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 on Windows 10 Version 1803 for 32-bit Systems	4507435 Security Update	Critical	Remote Code Execution	4503286	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 on Windows 10 Version 1803 for x64-based Systems	4507435 Security Update	Critical	Remote Code Execution	4503286	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-2019-1062						
Microsoft Edge on Windows 10 Version 1803 for ARM64-based Systems	4507435 Security Update	Critical	Remote Code Execution	4503286	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 on Windows 10 Version 1809 for 32-bit Systems	4507469 Security Update	Critical	Remote Code Execution	4503327	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 on Windows 10 Version 1809 for x64-based Systems	4507469 Security Update	Critical	Remote Code Execution	4503327	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-2019-1062						
Microsoft Edge on Windows 10 Version 1809 for ARM64-based Systems	4507469 Security Update	Critical	Remote Code Execution	4503327	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 on Windows Server 2019	4507469 Security Update	Moderate	Remote Code Execution	4503327	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 on Windows 10 Version 1709 for ARM64-based Systems	4507455 Security Update	Critical	Remote Code Execution	4503284	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 on Windows	4507453 Security Update	Critical	Remote Code Execution	4503293	Base: 4.2 Temporal: 3.8	Yes

CVE-2019-1062						
10 Version 1903 for 32-bit Systems					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 on Windows 10 Version 1903 for x64-based Systems	4507453 Security Update	Critical	Remote Code Execution	4503293	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 on Windows 10 Version 1903 for ARM64-based Systems	4507453 Security Update	Critical	Remote Code Execution	4503293	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	4503293	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1063 - Internet Explorer Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1063 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. 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.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by modifying how Internet Explorer handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1063						
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	4507434 IE Cumulative 4507452 Monthly Rollup	Moderate	Remote Code Execution	4503273	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 9 on Windows Server 2008 for x64-based Systems Service Pack 2	4507434 IE Cumulative 4507452 Monthly Rollup	Moderate	Remote Code Execution	4503273	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-2019-1063						
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1	4507434 IE Cumulative 4507449 Monthly Rollup	Critical	Remote Code Execution	4503292	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 7 for x64-based Systems Service Pack 1	4507434 IE Cumulative 4507449 Monthly Rollup	Critical	Remote Code Execution	4503292	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	4507434 IE Cumulative 4507449 Monthly	Moderate	Remote Code Execution	4503292	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-2019-1063						
Server 2008 R2 for x64-based Systems Service Pack 1	Rollup					
Internet Explorer 11 on Windows Server 2012	4507434 IE Cumulative	Moderate	Remote Code Execution	4503259	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	4507448 Monthly Rollup 4507434 IE Cumulative	Critical	Remote Code Execution	4503259	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	4507448 Monthly Rollup	Critical	Remote Code Execution	4503259	Base: 7.5 Temporal: 6.7	Yes

CVE-2019-1063						
Windows 8.1 for x64-based systems	4507434 IE Cumulative				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 2012 R2	4507448 Monthly Rollup 4507434 IE Cumulative	Moderate	Remote Code Execution	4503259	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	4507448 Monthly Rollup	Critical	Remote Code Execution	4503276	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	4507458 Security Update	Critical	Remote Code Execution	4503291	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-2019-1063						
Internet Explorer 11 on Windows 10 for x64-based Systems	4507458 Security Update	Critical	Remote Code Execution	4503291	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 2016	4507460 Security Update	Moderate	Remote Code Execution	4503267	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	4507460 Security Update	Critical	Remote Code Execution	4503267	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-2019-1063						
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4507460 Security Update	Critical	Remote Code Execution	4503267	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 32-bit Systems	4507450 Security Update	Critical	Remote Code Execution	4503279	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	4507450 Security Update	Critical	Remote Code Execution	4503279	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-2019-1063						
10 Version 1703 for x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems	4507455 Security Update	Critical	Remote Code Execution	4503284	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-	4507455 Security Update	Critical	Remote Code Execution	4503284	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-2019-1063						
based Systems						
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems	4507435 Security Update	Critical	Remote Code Execution	4503286	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	4507435 Security Update	Critical	Remote Code Execution	4503286	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-2019-1063						
Internet Explorer 11 on Windows 10 Version 1803 for ARM64-based Systems	4507435 Security Update	Critical	Remote Code Execution	4503286	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 32-bit Systems	4507469 Security Update	Critical	Remote Code Execution	4503327	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	4507469 Security Update	Critical	Remote Code Execution	4503327	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-2019-1063						
10 Version 1809 for x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems	4507469 Security Update	Critical	Remote Code Execution	4503327	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	4507469 Security Update	Moderate	Remote Code Execution	4503327	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-2019-1063						
Internet Explorer 11 on Windows 10 Version 1709 for ARM64-based Systems	4507455 Security Update	Critical	Remote Code Execution	4503284	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 32-bit Systems	4507453 Security Update	Critical	Remote Code Execution	4503293	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	4507453 Security Update	Critical	Remote Code Execution	4503293	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-2019-1063						
10 Version 1903 for x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1903 for ARM64-based Systems	4507453 Security Update	Critical	Remote Code Execution	4503293	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	4507462 Monthly Rollup 4507434 IE Cumulative	Moderate	Remote Code Execution	4503259	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-2019-1067 - Windows Kernel Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1067 MITRE NVD	**CVE Title:** Windows Kernel Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when the Windows kernel 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 to take control of an affected system. The update addresses the vulnerability by correcting how the Windows kernel handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1067						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	4507458 Security Update	Important	Elevation of Privilege	4503291	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-	4507458 Security Update	Important	Elevation of Privilege	4503291	Base: 7.8 Temporal: 7	Yes

CVE-2019-1067						
based Systems					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 2016	4507460 Security Update	Important	Elevation of Privilege	4503267	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	4507460 Security Update	Important	Elevation of Privilege	4503267	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	4507460 Security Update	Important	Elevation of Privilege	4503267	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)	4507460 Security Update	Important	Elevation of Privilege	4503267	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	4507450 Security Update	Important	Elevation of Privilege	4503279	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-2019-1067						
Windows 10 Version 1703 for x64-based Systems	4507450 Security Update	Important	Elevation of Privilege	4503279	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	4507455 Security Update	Important	Elevation of Privilege	4503284	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	4507455 Security Update	Important	Elevation of Privilege	4503284	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	4507435 Security Update	Important	Elevation of Privilege	4503286	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	4507435 Security Update	Important	Elevation of Privilege	4503286	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-2019-1067						
Windows Server, version 1803 (Server Core Installation)	4507435 Security Update	Important	Elevation of Privilege	4503286	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	4507435 Security Update	Important	Elevation of Privilege	4503286	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	4507469 Security Update	Important	Elevation of Privilege	4503327	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	4507469 Security Update	Important	Elevation of Privilege	4503327	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-2019-1067						
Windows 10 Version 1809 for ARM64-based Systems	4507469 Security Update	Important	Elevation of Privilege	4503327	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	4507469 Security Update	Important	Elevation of Privilege	4503327	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)	4507469 Security Update	Important	Elevation of Privilege	4503327	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	4507455 Security Update	Important	Elevation of Privilege	4503284	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	4507453 Security Update	Important	Elevation of Privilege	4503293	Base: 7.8 Temporal: 7	Yes

CVE-2019-1067						
1903 for 32-bit Systems					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 1903 for x64-based Systems	4507453 Security Update	Important	Elevation of Privilege	4503293	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	4507453 Security Update	Important	Elevation of Privilege	4503293	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)	4507453 Security Update	Important	Elevation of Privilege	4503293	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-2019-1068 - Microsoft SQL Server Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1068 MITRE NVD	**CVE Title:** Microsoft SQL Server Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in Microsoft SQL Server when it incorrectly handles processing of internal functions. An attacker who successfully exploited this vulnerability could execute code in the context of the SQL Server Database Engine service account. To exploit the vulnerability, an authenticated attacker would need to submit a specially crafted query to an affected SQL server. The security update addresses the vulnerability by modifying how the Microsoft SQL Server Database Engine handles the processing of functions. **FAQ:** **There are GDR and/or CU (Cumulative Update) updates offered for my version of SQL Server. How do I know which update to use?**	Important	Remote Code Execution

<table>
<tr><th>CVE ID</th><th>Vulnerability Description</th><th>Maximum Severity Rating</th><th>Vulnerability Impact</th></tr>
<tr><td></td><td>

First, determine your SQL Server version number. For more information on determining your SQL Server version number, see Microsoft Knowledge Base Article 321185 - How to determine the version, edition, and update level of SQL Server and its components.
Second, in the table below, locate your version number or the version range that your version number falls within. The corresponding update is the one you need to install.

Note If your SQL Server version number is not represented in the table below, your SQL Server version is no longer supported. Please upgrade to the latest Service Pack or SQL Server product in order to apply this and future security updates.
<table>
<tr><th>Update number</th><th>Title</th><th>Apply if current product version isâ€¦</th><th>This security update also includes servicing releases up throughâ€¦</th></tr>
<tr><td>4505217</td><td>Description of the security update for the Remote Code Execution vulnerability in SQL Server 2014 SP2 (GDR): June 11, 2019</td><td>12.0.5000.0 - 12.0.5214.6</td><td>KB4057120</td></tr>
</table>
</td><td></td><td></td></tr>
</table>

CVE ID	Vulnerability Description				Maximum Severity Rating	Vulnerability Impact
	4505419	Description of the security update for the Remote Code Execution vulnerability in SQL Server 2014 SP2 (CU+GDR: June 11, 2019	12.0.5511.0 - 12.0.5632.1	KB4491540 â€“ SQL14 SP2 CU17		
	4505218	Description of the security update for the Remote Code Execution vulnerability in SQL Server 2014 SP3 (GDR): June 11, 2019	12.0.6024.0	SP3		
	4505422	Description of the security update for the Remote Code Execution vulnerability in SQL Server 2014 SP3 (CU+GDR): June 11, 2019	12.0.6205.1 - 12.0.6259.0	KB4491539 â€“ SQL14 SP3 CU3		
	4505219	Description of the security update for the Remote Code Execution vulnerability in SQL Server 2016 SP1(GDR): June 11, 2019	13.0.4001.0 - 13.0.4224.16	KB4458842		
	4505221	Description of the security update for the Remote Code Execution vulnerability in SQL Server 2016 SP1 (CU+GDR): June 11, 2019	13.0.4411.0 - 13.0.4514.0	KB4495257 â€“ SQL16 SP1 CU115		

CVE ID	Vulnerability Description				Maximum Severity Rating	Vulnerability Impact
	4505220	Description of the security update for the Remote Code Execution vulnerability in SQL Server 2016 SP2 (GDR): June 11, 2019	13.0.5026.0 - 13.0.5081.1	KB4293802		
	4505222	Description of the security update for the Remote Code Execution vulnerability in SQL Server 2016 SP2 (CU+GDR): June 11, 2019	13.0.5149.0 - 13.0.5337.0	KB4495256 â€“ SQL SP2 CU7		
	4505224	Description of the security update for the Remote Code Execution vulnerability in SQL Server 2017 (GDR): June 11, 2019	14.0.1000.169 - 14.0.2014.14	KB4494351		
	4505225	Description of the security update for the Remote Code Execution vulnerability in SQL Server 2017 (CU+GDR): June 11, 2019	14.0.3006.16 - 14.0.3162.1	KB4498951 â€“ SQL17 RTM CU15		
	What are the GDR and CU update designations and how do they differ? The General Distribution Release (GDR) and Cumulative Update (CU) designations correspond to the two different servicing options in place for SQL Server baseline releases. A baseline can be either an RTM release or a Service Pack release.					

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	• GDR updates â€“ cumulatively only contain security updates for the given baseline. • CU updates â€“ cumulatively contain all functional fixes and security updates for the given baseline. For any given baseline, either the GDR or CU updates could be options (see below). • If SQL Server installation is at a baseline version, you can choose either the GDR or CU update. • If SQL Server installation has intentionally only installed past GDR updates, then choose to install the GDR update package. • If SQL Server installation has intentionally installed previous CU updates, then chose to install the CU security update package. • NOTE: You are allowed to make a change from GDR updates to CU updates ONE TIME. Once a SQL Server CU update is applied to a SQL Server installation, there is NO way to go back to the GDR update path. **Does this security update apply to SQL Server 2017 on Linux or on Linux Docker Containers?** Yes. For information on obtaining and installing the CU or GDR updates on Linux Operating Systems or Docker Containers, please see:		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	1. Configure repositories for installing and upgrading SQL Server on Linux 2. Release notes for SQL Server 2017 on Linux 3. Official images for Microsoft SQL Server on Linux for Docker Engine **Will these security updates be offered to SQL Server clusters?** Yes. The updates will also be offered to SQL Server 2016 SP1/SP2 and SQL Server 2017 RTM instances that are clustered. Updates for SQL Server clusters will require user interaction. If the SQL Server 2016 SP1/SP2 or SQL Server 2017 RTM cluster has a passive node, to reduce downtime, Microsoft recommends that you scan and apply the update to the inactive node first, then scan and apply it to the active node. When all components have been updated on all nodes, the update will no longer be offered. **Can the security updates be applied to SQL Server instances on Windows Azure (IaaS)?** Yes. SQL Server instances on Windows Azure (IaaS) can be offered the security updates through Microsoft Update, or customers can download the security updates from Microsoft Download Center and apply them manually. **Mitigations:**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Workarounds:** None **Revision:** 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1068						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SQL Server 2014 Service Pack 2 for 32-bit Systems (GDR)	4505217 Security Update	Important	Remote Code Execution	4057120	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1068						
Microsoft SQL Server 2014 Service Pack 2 for 32-bit Systems (CU+GDR)	4505419 Security Update	Important	Remote Code Execution	4057120	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SQL Server 2014 Service Pack 2 for x64-based Systems (CU+GDR)	4505419 Security Update	Important	Remote Code Execution	4057120	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SQL Server 2014 Service Pack 2 for x64-based Systems (GDR)	4505217 Security Update	Important	Remote Code Execution	4057120	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SQL Server 2016 for x64-based Systems Service Pack 1 (GDR)	4505219 Security Update	Important	Remote Code Execution	4293808	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SQL Server 2016 for x64-based Systems Service Pack 1 (CU+GDR)	4505221 Security Update	Important	Remote Code Execution	4293808	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SQL Server 2017 for x64-based Systems (GDR)	4505224 Security Update	Important	Remote Code Execution	4494351	Base: N/A Temporal:	Maybe

CVE-2019-1068						
					N/A Vector: N/A	
Microsoft SQL Server 2017 for x64-based Systems (CU+GDR)	4505225 Security Update	Important	Remote Code Execution	4494351	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SQL Server 2016 for x64-based Systems Service Pack 2 (CU+GDR)	4505222 Security Update	Important	Remote Code Execution	4494351	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SQL Server 2016 for x64-based Systems Service Pack 2 (GDR)	4505220 Security Update	Important	Remote Code Execution	4293802	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SQL Server 2014 Service Pack 3 for x64-based Systems (GDR)	4505218 Security Update	Important	Remote Code Execution	4293802	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SQL Server 2014 Service Pack 3 for x64-based Systems (CU+GDR)	4505422 Security Update	Important	Remote Code Execution	4293802	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1068						
Microsoft SQL Server 2014 Service Pack 3 for 32-bit Systems (GDR)	4505218 Security Update	Important	Remote Code Execution	4293802	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SQL Server 2014 Service Pack 3 for 32-bit Systems (CU+GDR)	4505422 Security Update	Important	Remote Code Execution	4293802	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1071 - Windows Kernel Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1071 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.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	An authenticated attacker could exploit this vulnerability by running a specially crafted application. 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 Kernel memory read - unintentional read access to memory contents in kernel space from a user mode process. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1071						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4507449 Monthly Rollup 4507456 Security Only	Important	Information Disclosure	4503292	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	4507449 Monthly Rollup 4507456 Security Only	Important	Information Disclosure	4503292	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	4507449 Monthly Rollup 4507456	Important	Information Disclosure	4503292	Base: 5.5 Temporal: 5 Vector:	Yes

CVE-2019-1071						
Systems Service Pack 1 (Server Core installation)	Security Only				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	4507449 Monthly Rollup 4507456 Security Only	Important	Information Disclosure	4503292	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	4507449 Monthly Rollup 4507456 Security Only	Important	Information Disclosure	4503292	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	4507452 Monthly	Important	Information Disclosure	4503273	Base: 5.5 Temporal: 5	Yes

CVE-2019-1071						
2008 for 32-bit Systems Service Pack 2 (Server Core installation)	Rollup 4507461 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 2012	4507462 Monthly Rollup 4507464 Security Only	Important	Information Disclosure	4503285	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)	4507462 Monthly Rollup 4507464 Security Only	Important	Information Disclosure	4503285	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	4507448 Monthly Rollup	Important	Information Disclosure	4503276	Base: 5.5 Temporal: 5 Vector:	Yes

CVE-2019-1071						
	4507457 Security Only				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	4507448 Monthly Rollup 4507457 Security Only	Important	Information Disclosure	4503276	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	4507448 Monthly Rollup 4507457 Security Only	Important	Information Disclosure	4503276	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	4507448 Monthly Rollup	Important	Information Disclosure	4503276	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	4507448 Monthly Rollup	Important	Information Disclosure	4503276	Base: 5.5 Temporal: 5 Vector:	Yes

CVE-2019-1071						
(Server Core installation)	4507457 Security Only				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 for 32-bit Systems	4507458 Security Update	Important	Information Disclosure	4503291	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	4507458 Security Update	Important	Information Disclosure	4503291	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	4507460 Security Update	Important	Information Disclosure	4503267	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 32-bit Systems	4507460 Security Update	Important	Information Disclosure	4503267	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-2019-1071						
Windows 10 Version 1607 for x64-based Systems	4507460 Security Update	Important	Information Disclosure	4503267	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)	4507460 Security Update	Important	Information Disclosure	4503267	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	4507450 Security Update	Important	Information Disclosure	4503279	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 x64-based Systems	4507450 Security Update	Important	Information Disclosure	4503279	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	4507455 Security	Important	Information Disclosure	4503284	Base: 5.5 Temporal: 5	Yes

CVE-2019-1071						
1709 for 32-bit 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 x64-based Systems	4507455 Security Update	Important	Information Disclosure	4503284	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	4507435 Security Update	Important	Information Disclosure	4503286	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	4507435 Security Update	Important	Information Disclosure	4503286	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 1803 (Server	4507435 Security Update	Important	Information Disclosure	4503286	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-2019-1071						
Core Installation)						
Windows 10 Version 1803 for ARM64-based Systems	4507435 Security Update	Important	Information Disclosure	4503286	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1809 for 32-bit Systems	4507469 Security Update	Important	Information Disclosure	4503327	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	4507469 Security Update	Important	Information Disclosure	4503327	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-	4507469 Security Update	Important	Information Disclosure	4503327	Base: 5.5 Temporal: 5 Vector:	Yes

CVE-2019-1071						
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 Server 2019	4507469 Security Update	Important	Information Disclosure	4503327	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)	4507469 Security Update	Important	Information Disclosure	4503327	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-based Systems	4507455 Security Update	Important	Information Disclosure	4503284	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	4507453 Security Update	Important	Information Disclosure	4503293	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-1071						
32-bit Systems						
Windows 10 Version 1903 for x64-based Systems	4507453 Security Update	Important	Information Disclosure	4503293	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1903 for ARM64-based Systems	4507453 Security Update	Important	Information Disclosure	4503293	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server, version 1903 (Server Core installation)	4507453 Security Update	Important	Information Disclosure	4503293	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2008 for	4507452 Monthly Rollup	Important	Information Disclosure	4503273	Base: 5.5 Temporal: 5 Vector:	Yes

CVE-2019-1071						
Itanium-Based Systems Service Pack 2	4507461 Security Only				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 for 32-bit Systems Service Pack 2	4507452 Monthly Rollup 4507461 Security Only	Important	Information Disclosure	4503273	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 Service Pack 2	4507452 Monthly Rollup 4507461 Security Only	Important	Information Disclosure	4503273	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	4507452 Monthly Rollup 4507461	Important	Information Disclosure	4503273	Base: 5.5 Temporal: 5 Vector:	Yes

CVE-2019-1071						
Systems Service Pack 2 (Server Core installation)	Security Only				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	

CVE-2019-1072 - Azure DevOps Server and Team Foundation Server Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1072 MITRE NVD	**CVE Title:** Azure DevOps Server and Team Foundation Server Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when Azure DevOps Server and Team Foundation Server (TFS) improperly handle user input. An attacker who successfully exploited the vulnerability could execute code on the target server in the context of the DevOps or TFS service account.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	To exploit the vulnerability, an attacker could submit a specially crafted file to an affected server. If anonymous access is allowed to projects on an affected server, the attacker would not require authentication. The update corrects the way that DevOps Server and TFS process certain file types. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 07/09/2019 07:00:00 Information published. 2.0 07/09/2019 07:00:00 Added Team Foundation Server 2010 SP1 (x86) and Team Foundation Server 2010 SP1 (x64) to the Security Updates table as there are unique security updates for each architecture. Corrected Security Update download links for Team Foundation Server 2012 Update 4, Team Foundation Server 2013 Update 5, and Azure DevOps Server 2019.0.1.		

Affected Software

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

CVE-2019-1072						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Team Foundation Server 2012 Update 4	Release Notes Security Update	Critical	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	Maybe
Team Foundation Server 2013 Update 5	Release Notes Security Update	Critical	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	Maybe
Team Foundation Server 2018 Update 1.2	Release Notes Security Update	Critical	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	Maybe
Team Foundation Server 2017 Update 3.1	Release Notes Security Update	Critical	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1072						
Team Foundation Server 2018 Update 3.2	Release Notes Security Update	Critical	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	Maybe
Team Foundation Server 2015 Update 4.2	Release Notes Security Update	Critical	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	Maybe
Azure DevOps Server 2019.0.1	Release Notes Security Update	Critical	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	Maybe
Team Foundation Server 2010 SP1 (x86)	Release Notes Security Update	Critical	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	Maybe
Team Foundation Server 2010 SP1 (x64)	Release Notes Security Update	Critical	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1073 - Windows Kernel Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1073 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 Kernel memory read - unintentional read access to memory contents in kernel space from a user mode process. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1073						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4507449 Monthly Rollup 4507456 Security Only	Important	Information Disclosure	4503292	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	4507449 Monthly Rollup 4507456 Security Only	Important	Information Disclosure	4503292	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	4507449 Monthly Rollup 4507456 Security Only	Important	Information Disclosure	4503292	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-2019-1073						
Core installation)						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4507449 Monthly Rollup 4507456 Security Only	Important	Information Disclosure	4503292	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	4507449 Monthly Rollup 4507456 Security Only	Important	Information Disclosure	4503292	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	4507452 Monthly Rollup 4507461 Security Only	Important	Information Disclosure	4503273	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-2019-1073						
Pack 2 (Server Core installation)						
Windows Server 2012	4507462 Monthly Rollup 4507464 Security Only	Important	Information Disclosure	4503285	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)	4507462 Monthly Rollup 4507464 Security Only	Important	Information Disclosure	4503285	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	4507448 Monthly Rollup 4507457 Security Only	Important	Information Disclosure	4503276	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-2019-1073						
Windows 8.1 for x64-based systems	4507448 Monthly Rollup 4507457 Security Only	Important	Information Disclosure	4503276	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	4507448 Monthly Rollup 4507457 Security Only	Important	Information Disclosure	4503276	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	4507448 Monthly Rollup	Important	Information Disclosure	4503276	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 (Server Core installation)	4507448 Monthly Rollup 4507457 Security Only	Important	Information Disclosure	4503276	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-2019-1073						
Windows 10 for 32-bit Systems	4507458 Security Update	Important	Information Disclosure	4503291	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	4507458 Security Update	Important	Information Disclosure	4503291	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	4507460 Security Update	Important	Information Disclosure	4503267	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 32-bit Systems	4507460 Security Update	Important	Information Disclosure	4503267	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	4507460 Security Update	Important	Information Disclosure	4503267	Base: 5.5 Temporal: 5 Vector:	Yes

CVE-2019-1073						
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 Server 2016 (Server Core installation)	4507460 Security Update	Important	Information Disclosure	4503267	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	4507450 Security Update	Important	Information Disclosure	4503279	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 x64-based Systems	4507450 Security Update	Important	Information Disclosure	4503279	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 32-bit Systems	4507455 Security Update	Important	Information Disclosure	4503284	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-2019-1073						
Windows 10 Version 1709 for x64-based Systems	4507455 Security Update	Important	Information Disclosure	4503284	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	4507435 Security Update	Important	Information Disclosure	4503286	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	4507435 Security Update	Important	Information Disclosure	4503286	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 1803 (Server Core Installation)	4507435 Security Update	Important	Information Disclosure	4503286	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-2019-1073						
Windows 10 Version 1803 for ARM64-based Systems	4507435 Security Update	Important	Information Disclosure	4503286	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	4507469 Security Update	Important	Information Disclosure	4503327	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	4507469 Security Update	Important	Information Disclosure	4503327	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	4507469 Security Update	Important	Information Disclosure	4503327	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-2019-1073						
Windows Server 2019	4507469 Security Update	Important	Information Disclosure	4503327	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)	4507469 Security Update	Important	Information Disclosure	4503327	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-based Systems	4507455 Security Update	Important	Information Disclosure	4503284	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	4507453 Security Update	Important	Information Disclosure	4503293	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-2019-1073						
Windows 10 Version 1903 for x64-based Systems	4507453 Security Update	Important	Information Disclosure	4503293	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	4507453 Security Update	Important	Information Disclosure	4503293	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 Core installation)	4507453 Security Update	Important	Information Disclosure	4503293	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 Itanium-Based	4507452 Monthly Rollup 4507461 Security	Important	Information Disclosure	4503273	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-2019-1073						
Systems Service Pack 2	Only					
Windows Server 2008 for 32-bit Systems Service Pack 2	4507452 Monthly Rollup 4507461 Security Only	Important	Information Disclosure	4503273	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 Service Pack 2	4507452 Monthly Rollup 4507461 Security Only	Important	Information Disclosure	4503273	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 Service	4507452 Monthly Rollup 4507461 Security Only	Important	Information Disclosure	4503273	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-2019-1073						
Pack 2 (Server Core installation)						

CVE-2019-1074 - Microsoft Windows Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1074 MITRE NVD	**CVE Title:** Microsoft Windows Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in Microsoft Windows where certain folders, with local service privilege, are vulnerable to symbolic link attack. An attacker who successfully exploited this vulnerability could potentially access unauthorized information. The update addresses this vulnerability by not allowing symbolic links in these scenarios. **FAQ:** None	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1074						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1709 for 32-bit Systems	4507455 Security Update	Important	Elevation of Privilege	4503284	Base: 5.3 Temporal: 5.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:L	Yes

CVE-2019-1074						
Windows 10 Version 1709 for x64-based Systems	4507455 Security Update	Important	Elevation of Privilege	4503284	Base: 5.3 Temporal: 5.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:L	Yes
Windows 10 Version 1803 for 32-bit Systems	4507435 Security Update	Important	Elevation of Privilege	4503286	Base: 5.3 Temporal: 5.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:L	Yes
Windows 10 Version 1803 for x64-based Systems	4507435 Security Update	Important	Elevation of Privilege	4503286	Base: 5.3 Temporal: 5.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:L	Yes
Windows Server, version 1803 (Server Core Installation)	4507435 Security Update	Important	Elevation of Privilege	4503286	Base: 5.3 Temporal: 5.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:L	Yes
Windows 10 Version 1803 for ARM64-based Systems	4507435 Security Update	Important	Elevation of Privilege	4503286	Base: 5.3 Temporal: 5.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:L	Yes
Windows 10 Version 1809 for 32-bit Systems	4507469 Security Update	Important	Elevation of Privilege	4503327	Base: 5.3 Temporal: 5.3	Yes

CVE-2019-1074						
					Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:L	
Windows 10 Version 1809 for x64-based Systems	4507469 Security Update	Important	Elevation of Privilege	4503327	Base: 5.3 Temporal: 5.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:L	Yes
Windows 10 Version 1809 for ARM64-based Systems	4507469 Security Update	Important	Elevation of Privilege	4503327	Base: 5.3 Temporal: 5.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:L	Yes
Windows Server 2019	4507469 Security Update	Important	Elevation of Privilege	4503327	Base: 5.3 Temporal: 5.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:L	Yes
Windows Server 2019 (Server Core installation)	4507469 Security Update	Important	Elevation of Privilege	4503327	Base: 5.3 Temporal: 5.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:L	Yes
Windows 10 Version 1709 for ARM64-based Systems	4507455 Security Update	Important	Elevation of Privilege	4503284	Base: 5.3 Temporal: 5.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:L	Yes

CVE-2019-1074						
Windows 10 Version 1903 for 32-bit Systems	4507453 Security Update	Important	Elevation of Privilege	4503293	Base: 5.3 Temporal: 5.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:L	Yes
Windows 10 Version 1903 for x64-based Systems	4507453 Security Update	Important	Elevation of Privilege	4503293	Base: 5.3 Temporal: 5.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:L	Yes
Windows 10 Version 1903 for ARM64-based Systems	4507453 Security Update	Important	Elevation of Privilege	4503293	Base: 5.3 Temporal: 5.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:L	Yes
Windows Server, version 1903 (Server Core installation)	4507453 Security Update	Important	Elevation of Privilege	4503293	Base: 5.3 Temporal: 5.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:L	Yes

CVE-2019-1075 - ASP.NET Core Spoofing Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1075 MITRE NVD	**CVE Title:** ASP.NET Core Spoofing Vulnerability **Description:** A spoofing vulnerability exists in ASP.NET Core that could lead to an open redirect. An attacker who successfully exploited the vulnerability could redirect a targeted user to a malicious website. To exploit the vulnerability, an attacker could send a link that has a specially crafted URL, and convince the user to click the link. The update addresses the vulnerability by correcting how ASP.NET Core parses URLs. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 07/09/2019 07:00:00	Moderate	Spoofing

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-2019-1075						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
ASP.NET Core 2.1	Release Notes Security Update	Moderate	Spoofing		Base: N/A Temporal: N/A Vector: N/A	Maybe
ASP.NET Core 2.2	Release Notes Security Update	Moderate	Spoofing		Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1076 - Team Foundation Server Cross-site Scripting Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1076 MITRE NVD	**CVE Title:** Team Foundation Server Cross-site Scripting Vulnerability **Description:** A Cross-site Scripting (XSS) vulnerability exists when Team Foundation Server does not properly sanitize user provided input. An authenticated attacker could exploit the vulnerability by sending a specially crafted payload to the Team Foundation Server, which will get executed in the context of the user every time a user visits the compromised page. 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, execute malicious code, and use the victim's identity to take actions on the site on behalf of the user, such as change permissions and delete content. The security update addresses the vulnerability by ensuring that Team Foundation Server sanitizes user inputs.	Important	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.1 07/09/2019 07:00:00 Corrected the Security Update download link Azure DevOps Server 2019.0.1. 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1076						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Team Foundation Server 2018 Update 3.2	Release Notes Security Update	Important	Spoofing		Base: N/A Temporal: N/A Vector: N/A	Maybe
Azure DevOps Server 2019.0.1	Release Notes Security Update	Important	Spoofing		Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1077 - Visual Studio Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1077 MITRE NVD	**CVE Title:** Visual Studio Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when the Visual Studio updater service improperly handles file permissions. An attacker who successfully exploited this vulnerability overwrite arbitrary files with XML content in the security context of the local system.	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. The update addresses the vulnerability by correcting how the Visual Studio updater handles permissions. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1077						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Visual Studio 2017 version 15.9	Release Notes Security Update	Important	Elevation of Privilege		Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Visual Studio 2019 version 16.0	Release Notes Security Update	Important	Elevation of Privilege		Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Visual Studio 2019 version 16.1	Release Notes Security Update	Important	Elevation of Privilege		Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1079 - Visual Studio Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1079 MITRE NVD	**CVE Title:** Visual Studio Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when Visual Studio improperly parses XML input in certain settings files. An attacker who successfully exploited this vulnerability could read arbitrary files via an XML external entity (XXE) declaration. To exploit the vulnerability, an attacker could create specially crafted XML data and convince an authenticated user to open the file. The update addresses the vulnerability by modifying the way that Visual Studio parses XML 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 unauthorized file system access - reading from the file system.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1079						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Visual Studio 2010 Service Pack 1	4506161 Security Update	Important	Information Disclosure		Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1079						
Microsoft Visual Studio 2012 Update 5	4506162 Security Update	Important	Information Disclosure		Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Visual Studio 2013 Update 5	4506163 Security Update	Important	Information Disclosure		Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Visual Studio 2015 Update 3	4506164 Security Update	Important	Information Disclosure		Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1082 - Microsoft Windows Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1082	**CVE Title:** Microsoft Windows Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in Microsoft Windows where a certain dll, with Local Service privilege, is vulnerable to race planting a customized dll.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	An attacker who successfully exploited this vulnerability could potentially elevate privilege to SYSTEM. The update addresses this vulnerability by requiring system privileges for a certain DLL. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1082						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4507449 Monthly Rollup 4507456 Security Only	Important	Elevation of Privilege	4503292	Base: 7.7 Temporal: 7.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L	Yes
Windows 7 for x64-based Systems Service Pack 1	4507449 Monthly Rollup 4507456 Security Only	Important	Elevation of Privilege	4503292	Base: 7.7 Temporal: 7.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4507449 Monthly Rollup 4507456 Security Only	Important	Elevation of Privilege	4503292	Base: 7.7 Temporal: 7.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L	Yes
Windows Server 2008 R2 for Itanium-Based	4507449 Monthly Rollup	Important	Elevation of Privilege	4503292	Base: 7.7 Temporal: 7.7	Yes

CVE-2019-1082						
Systems Service Pack 1	4507456 Security Only				Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L	
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4507449 Monthly Rollup 4507456 Security Only	Important	Elevation of Privilege	4503292	Base: 7.7 Temporal: 7.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L	Yes
Windows Server 2012	4507462 Monthly Rollup 4507464 Security Only	Important	Elevation of Privilege	4503285	Base: 7.7 Temporal: 7.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L	Yes
Windows Server 2012 (Server Core installation)	4507462 Monthly Rollup 4507464 Security Only	Important	Elevation of Privilege	4503285	Base: 7.7 Temporal: 7.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L	Yes

CVE-2019-1082						
Windows 8.1 for 32-bit systems	4507448 Monthly Rollup 4507457 Security Only	Important	Elevation of Privilege	4503276	Base: 7.7 Temporal: 7.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L	Yes
Windows 8.1 for x64-based systems	4507448 Monthly Rollup 4507457 Security Only	Important	Elevation of Privilege	4503276	Base: 7.7 Temporal: 7.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L	Yes
Windows Server 2012 R2	4507448 Monthly Rollup 4507457 Security Only	Important	Elevation of Privilege	4503276	Base: 7.7 Temporal: 7.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L	Yes
Windows RT 8.1	4507448 Monthly Rollup	Important	Elevation of Privilege	4503276	Base: 7.7 Temporal: 7.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L	Yes

CVE-2019-1082						
Windows Server 2012 R2 (Server Core installation)	4507448 Monthly Rollup 4507457 Security Only	Important	Elevation of Privilege	4503276	Base: 7.7 Temporal: 7.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L	Yes
Windows 10 for 32-bit Systems	4507458 Security Update	Important	Elevation of Privilege	4503291	Base: 7.7 Temporal: 7.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L	Yes
Windows 10 for x64-based Systems	4507458 Security Update	Important	Elevation of Privilege	4503291	Base: 7.7 Temporal: 7.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L	Yes
Windows Server 2016	4507460 Security Update	Important	Elevation of Privilege	4503267	Base: 7.7 Temporal: 7.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L	Yes
Windows 10 Version 1607 for 32-bit Systems	4507460 Security Update	Important	Elevation of Privilege	4503267	Base: 7.7 Temporal: 7.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L	Yes

CVE-2019-1082						
Windows 10 Version 1607 for x64-based Systems	4507460 Security Update	Important	Elevation of Privilege	4503267	Base: 7.7 Temporal: 7.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L	Yes
Windows Server 2016 (Server Core installation)	4507460 Security Update	Important	Elevation of Privilege	4503267	Base: 7.7 Temporal: 7.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L	Yes

CVE-2019-1083 - .NET Denial of Service Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1083 MITRE NVD	**CVE Title:** .NET Denial of Service Vulnerability **Description:** A denial of service vulnerability exists when Microsoft Common Object Runtime Library improperly handles web requests. An attacker who successfully exploited this vulnerability could cause a denial of service against a .NET web application.	Important	Denial of Service

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	A remote unauthenticated attacker could exploit this vulnerability by issuing specially crafted requests to the .NET application. The update addresses the vulnerability by correcting how the .NET web application handles web requests. **FAQ:** **There are two updates for .NET Framework 3.5 installed on Windows 10 version 1809 and Windows Server 2019. How do I know which update I need to install?** The security updates for Windows 10 version 1809 and Windows Server 2019 include both .NET Framework 3.5 and 4.7.2 or 4.8. Customers running these versions of Windows 10 need to determine if they are also running .NET Framework 4.7.2 or .NET Framework 4.8. Install the security update that includes that second version of .NET Framework. **Mitigations:** None **Workarounds:** None		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1083						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft .NET Framework 4.5.2 on Windows 7 for 32-bit Systems Service Pack 1	4507420 Monthly Rollup 4507411 Security Only	Important	Denial of Service	4503865	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows 7 for x64-based Systems Service Pack 1	4507420 Monthly	Important	Denial of Service	4503865	Base: N/A Temporal:	Maybe

CVE-2019-1083						
	Rollup 4507411 Security Only				N/A Vector: N/A	
Microsoft .NET Framework 4.5.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4507420 Monthly Rollup 4507411 Security Only	Important	Denial of Service	4503865	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4507420 Monthly Rollup 4507411 Security Only	Important	Denial of Service	4503865	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2012	4507412 Security Only 4507421 Monthly Rollup	Important	Denial of Service	4499407; 4503866	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1083						
Microsoft .NET Framework 4.5.2 on Windows Server 2012 (Server Core installation)	4507412 Security Only 4507421 Monthly Rollup	Important	Denial of Service	4499407; 4503866	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows 8.1 for 32-bit systems	4507413 Security Only 4507422 Monthly Rollup	Important	Denial of Service	4499408; 4503867	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows 8.1 for x64-based systems	4507413 Security Only 4507422 Monthly Rollup	Important	Denial of Service	4499408; 4503867	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2012 R2	4507413 Security Only 4507422 Monthly	Important	Denial of Service	4499408; 4503867	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1083						
	Rollup					
Microsoft .NET Framework 4.5.2 on Windows RT 8.1	4507422 Monthly Rollup	Important	Denial of Service	4499408; 4503867	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2012 R2 (Server Core installation)	4507413 Security Only 4507422 Monthly Rollup	Important	Denial of Service	4499408; 4503867	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2008 for 32-bit Systems Service Pack 2	4507423 Monthly Rollup 4507414 Security Only	Important	Denial of Service	4489489; 4499409	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2008 for x64-based Systems Service Pack 2	4507423 Monthly Rollup 4507414 Security	Important	Denial of Service	4489489; 4499409	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1083						
	Only					
Microsoft .NET Framework 4.6 on Windows Server 2008 for 32-bit Systems Service Pack 2	4507423 Monthly Rollup 4507414 Security Only	Important	Denial of Service	4489489; 4499409	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6 on Windows Server 2008 for x64-based Systems Service Pack 2	4507423 Monthly Rollup 4507414 Security Only	Important	Denial of Service	4489489; 4499409	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2 on Windows 10 for 32-bit Systems	4507458 Security Update	Important	Denial of Service	4503291	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.6/4.6.1/4.6.2 on Windows 10 for x64-based Systems	4507458 Security Update	Important	Denial of Service	4503291	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-1083						
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 7 for 32-bit Systems Service Pack 1	4507420 Monthly Rollup 4507411 Security Only	Important	Denial of Service	4503291	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 7 for x64-based Systems Service Pack 1	4507420 Monthly Rollup 4507411 Security Only	Important	Denial of Service	4503291	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4507420 Monthly Rollup 4507411 Security Only	Important	Denial of Service	4503291	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4507420 Monthly Rollup 4507411 Security	Important	Denial of Service	4503291	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1083						
	Only					
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012	4507421 Monthly Rollup 4507412 Security Only	Important	Denial of Service	4499407; 4503866	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012 (Server Core installation)	4507421 Monthly Rollup 4507412 Security Only	Important	Denial of Service	4499407; 4503866	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 8.1 for 32-bit systems	4507413 Security Only 4507422 Monthly Rollup	Important	Denial of Service	4499408; 4503867	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 8.1 for x64-based systems	4507422 Monthly Rollup 4507413	Important	Denial of Service	4499408; 4503867	Base: N/A Temporal: N/A	Maybe

CVE-2019-1083						
	Security Only				Vector: N/A	
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012 R2	4507422 Monthly Rollup 4507413 Security Only	Important	Denial of Service	4499408; 4503867	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows RT 8.1	4507422 Monthly Rollup	Important	Denial of Service	4499408; 4503867	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012 R2 (Server Core installation)	4507422 Monthly Rollup 4507413 Security Only	Important	Denial of Service	4499408; 4503867	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 7 for 32-bit Systems Service Pack 1	4507420 Monthly Rollup 4507411	Important	Denial of Service	4499406; 4503865	Base: N/A Temporal: N/A	Maybe

CVE-2019-1083						
	Security Only				Vector: N/A	
Microsoft .NET Framework 4.8 on Windows 7 for x64-based Systems Service Pack 1	4507420 Monthly Rollup 4507411 Security Only	Important	Denial of Service	4499406; 4503865	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4507420 Monthly Rollup 4507411 Security Only	Important	Denial of Service	4499406; 4503865	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4507420 Monthly Rollup 4507411 Security Only	Important	Denial of Service	4499406; 4503865	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2012	4507421 Monthly Rollup	Important	Denial of Service	4499407; 4503866	Base: N/A Temporal: N/A	Maybe

CVE-2019-1083						
	4507412 Security Only				Vector: N/A	
Microsoft .NET Framework 4.8 on Windows Server 2012 (Server Core installation)	4507421 Monthly Rollup 4507412 Security Only	Important	Denial of Service	4499407; 4503866	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 8.1 for 32-bit systems	4507422 Monthly Rollup 4507413 Security Only	Important	Denial of Service	4499408; 4503867	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 8.1 for x64-based systems	4507422 Monthly Rollup 4507413 Security Only	Important	Denial of Service	4499408; 4503867	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2012 R2	4507422 Monthly	Important	Denial of Service	4499408; 4503867	Base: N/A Temporal:	Maybe

CVE-2019-1083						
	Rollup 4507413 Security Only				N/A Vector: N/A	
Microsoft .NET Framework 4.8 on Windows RT 8.1	4507422 Monthly Rollup	Important	Denial of Service	4499408; 4503867	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2012 R2 (Server Core installation)	4507422 Monthly Rollup 4507413 Security Only	Important	Denial of Service	4499408; 4503867	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2016	4506986 Security Update	Important	Denial of Service	4495610; 4502560	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1607 for 32-bit Systems	4506986 Security Update	Important	Denial of Service	4495610; 4502560	Base: N/A Temporal: N/A	Maybe

CVE-2019-1083						
					Vector: N/A	
Microsoft .NET Framework 4.8 on Windows 10 Version 1607 for x64-based Systems	4506986 Security Update	Important	Denial of Service	4495610; 4502560	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2016 (Server Core installation)	4506986 Security Update	Important	Denial of Service	4495610; 4502560	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1703 for 32-bit Systems	4506987 Security Update	Important	Denial of Service	4495611; 4502561	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1703 for x64-based Systems	4506986 Security Update	Important	Denial of Service	4495610; 4502560	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1083						
Microsoft .NET Framework 4.8 on Windows 10 Version 1709 for 32-bit Systems	4506988 Security Update	Important	Denial of Service	4495613; 4502562	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1709 for x64-based Systems	4506986 Security Update	Important	Denial of Service	4495610; 4502560	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1803 for 32-bit Systems	4506989 Security Update	Important	Denial of Service	4495616; 4502563	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1803 for x64-based Systems	4506989 Security Update	Important	Denial of Service	4495616; 4502563	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server, version 1803 (Server Core Installation)	4506989 Security Update	Important	Denial of Service	4495616; 4502563	Base: N/A Temporal: N/A	Maybe

CVE-2019-1083						
					Vector: N/A	
Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 1809 for 32-bit Systems	4507419 Security Update	Important	Denial of Service	4486553; 4499405; 4503864	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 1809 for x64-based Systems	4507419 Security Update	Important	Denial of Service	4486553; 4499405; 4503864	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 AND 4.8 on Windows Server 2019	4507419 Security Update	Important	Denial of Service	4486553; 4499405; 4503864	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 AND 4.8 on Windows Server 2019 (Server Core installation)	4507419 Security Update	Important	Denial of Service	4486553; 4499405; 4503864	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1083						
Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 1903 for 32-bit Systems	4506991 Security Update	Important	Denial of Service	4495620; 4502584	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 1903 for x64-based Systems	4506991 Security Update	Important	Denial of Service	4495620; 4502584	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 AND 4.8 on Windows Server, version 1903 (Server Core installation)	4506991 Security Update	Important	Denial of Service	4495620; 4502584	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 AND 4.7.2 on Windows 10 Version 1809 for 32-bit Systems	4507419 Security Update	Important	Denial of Service	4486553; 4499405; 4503864	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 AND 4.7.2 on Windows 10 Version 1809 for x64-based Systems	4507419 Security Update	Important	Denial of Service	4486553; 4499405; 4503864	Base: N/A Temporal: N/A	Maybe

CVE-2019-1083						
					Vector: N/A	
Microsoft .NET Framework 3.5 AND 4.7.2 on Windows Server 2019	4507419 Security Update	Important	Denial of Service	4486553; 4499405; 4503864	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 AND 4.7.2 on Windows Server 2019 (Server Core installation)	4507419 Security Update	Important	Denial of Service	4486553; 4499405; 4503864	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2012	4507412 Security Only 4507421 Monthly Rollup	Important	Denial of Service	4499407; 4503866	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2012 (Server Core installation)	4507412 Security Only 4507421 Monthly	Important	Denial of Service	4499407; 4503866	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1083						
	Rollup					
Microsoft .NET Framework 3.5 on Windows 8.1 for 32-bit systems	4507413 Security Only 4507422 Monthly Rollup	Important	Denial of Service	4499408; 4503867	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows 8.1 for x64-based systems	4507413 Security Only 4507422 Monthly Rollup	Important	Denial of Service	4499408; 4503867	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2012 R2	4507413 Security Only 4507422 Monthly Rollup	Important	Denial of Service	4499408; 4503867	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2012 R2 (Server Core installation)	4507413 Security Only 4507422	Important	Denial of Service	4499408; 4503867	Base: N/A Temporal: N/A	Maybe

CVE-2019-1083						
	Monthly Rollup				Vector: N/A	
Microsoft .NET Framework 3.5 on Windows 10 for 32-bit Systems	4507458 Security Update	Important	Denial of Service	4503291	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 for x64-based Systems	4507458 Security Update	Important	Denial of Service	4503291	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows Server 2016	4507460 Security Update	Important	Denial of Service	4503267	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1607 for 32-bit Systems	4507460 Security Update	Important	Denial of Service	4503267	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-1083						
Microsoft .NET Framework 3.5 on Windows 10 Version 1607 for x64-based Systems	4507460 Security Update	Important	Denial of Service	4503267	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows Server 2016 (Server Core installation)	4507460 Security Update	Important	Denial of Service	4503267	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1703 for 32-bit Systems	4507450 Security Update	Important	Denial of Service	4503279	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1703 for x64-based Systems	4507450 Security Update	Important	Denial of Service	4503279	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1709 for 32-bit Systems	4507455 Security Update	Important	Denial of Service	4503284	Base: N/A Temporal: N/A	Yes

CVE-2019-1083						
					Vector: N/A	
Microsoft .NET Framework 3.5 on Windows 10 Version 1709 for x64-based Systems	4507455 Security Update	Important	Denial of Service	4503284	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1803 for 32-bit Systems	4507435 Security Update	Important	Denial of Service	4503286	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1803 for x64-based Systems	4507435 Security Update	Important	Denial of Service	4503286	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows Server, version 1803 (Server Core Installation)	4507435 Security Update	Important	Denial of Service	4503286	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-1083						
Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for Itanium-Based Systems Service Pack 2	4507414 Security Only 4507423 Monthly Rollup	Important	Denial of Service	4499409; 4503868	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for 32-bit Systems Service Pack 2	4507414 Security Only 4507423 Monthly Rollup	Important	Denial of Service	4499409; 4503868	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for x64-based Systems Service Pack 2	4507414 Security Only 4507423 Monthly Rollup	Important	Denial of Service	4499409; 4503868	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 2.0 Service Pack 2 on Windows Server 2008 for Itanium-Based Systems Service Pack 2	4507414 Security Only 4507423 Monthly	Important	Denial of Service	4499409; 4503868	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1083						
	Rollup					
Microsoft .NET Framework 2.0 Service Pack 2 on Windows Server 2008 for 32-bit Systems Service Pack 2	4507414 Security Only 4507423 Monthly Rollup	Important	Denial of Service	4499409; 4503868	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 2.0 Service Pack 2 on Windows Server 2008 for x64-based Systems Service Pack 2	4507414 Security Only 4507423 Monthly Rollup	Important	Denial of Service	4499409; 4503868	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5.1 on Windows 7 for 32-bit Systems Service Pack 1	4507411 Security Only 4507420 Monthly Rollup	Important	Denial of Service	4499406; 4503865	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5.1 on Windows 7 for x64-based Systems Service Pack 1	4507411 Security Only 4507420	Important	Denial of Service	4499406; 4503865	Base: N/A Temporal: N/A	Maybe

CVE-2019-1083						
	Monthly Rollup				Vector: N/A	
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4507411 Security Only 4507420 Monthly Rollup	Important	Denial of Service	4499406; 4503865	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4507411 Security Only 4507420 Monthly Rollup	Important	Denial of Service	4499406; 4503865	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4507411 Security Only 4507420 Monthly Rollup	Important	Denial of Service	4499406; 4503865	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1084 - Microsoft Exchange Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1084 MITRE NVD	**CVE Title:** Microsoft Exchange Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when Exchange allows creation of entities with Display Names having non-printable characters. An authenticated attacker could exploit this vulnerability by creating entities with invalid display names, which, when added to conversations, remain invisible. This security update addresses the issue by validating display names upon creation in Microsoft Exchange, and by rendering invalid display names correctly in Microsoft Outlook clients. **FAQ:** **What type of information could be disclosed by this vulnerability?**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	This vulnerability discloses email conversations and chats to unintended recipients. Entities created by exploiting this vulnerability can also be given access to documents via Sharepoint. **Is the Preview Pane an attack vector for this vulnerability?** No, the Preview Pane is not an attack vector. **Are the updates for the Microsoft Office for Mac and Outlook for iOS currently available?** The security update for Microsoft Office 2016 for Mac, Microsoft Office 2019 for Mac, and Outlook for iOS are not immediately available. The updates will be released as soon as possible, and when they are available, customers will be notified via a revision to this CVE information. **Mitigations:** None **Workarounds:** None		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1084						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Exchange Server 2010 Service Pack 3	4509410 Security Update	Important	Information Disclosure	4503028	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Outlook 2010 Service Pack 2 (32-bit editions)	4475509 Security Update	Important	Information Disclosure	4461623	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1084						
Microsoft Outlook 2010 Service Pack 2 (64-bit editions)	4475509 Security Update	Important	Information Disclosure	4461623	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2013 Service Pack 1 (32-bit editions)	4464558 Security Update	Important	Information Disclosure	4464504	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2013 Service Pack 1 (64-bit editions)	4464558 Security Update	Important	Information Disclosure	4464504	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2013 RT Service Pack 1	4464558 Security Update	Important	Information Disclosure	4464504	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Lync 2013 Service Pack 1 (32-bit)	4475519 Security Update	Important	Information Disclosure	4461487	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Lync Basic 2013 Service Pack 1 (32-bit)	4475519 Security Update	Important	Information Disclosure	4461487	Base: N/A Temporal:	Maybe

CVE-2019-1084						
					N/A Vector: N/A	
Microsoft Lync 2013 Service Pack 1 (64-bit)	4475519 Security Update	Important	Information Disclosure	4461487	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Lync Basic 2013 Service Pack 1 (64-bit)	4475519 Security Update	Important	Information Disclosure	4461487	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Outlook for Android	Release Notes Security Update	Important	Information Disclosure	4461487	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 for Mac		Important	Information Disclosure	4461487	Base: N/A Temporal: N/A Vector: N/A	
Microsoft Office 2016 (32-bit edition)	4475514 Security Update	Important	Information Disclosure	4011622	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1084						
Microsoft Office 2016 (64-bit edition)	4475514 Security Update	Important	Information Disclosure	4011622	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Outlook 2016 (32-bit edition)	4475517 Security Update	Important	Information Disclosure	4461601	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Outlook 2016 (64-bit edition)	4475517 Security Update	Important	Information Disclosure	4461601	Base: N/A Temporal: N/A Vector: N/A	Maybe
Skype for Business 2016 (32-bit)	4475545 Security Update	Important	Information Disclosure	4461473	Base: N/A Temporal: N/A Vector: N/A	Maybe
Skype for Business 2016 (64-bit)	4475545 Security Update	Important	Information Disclosure	4461473	Base: N/A Temporal: N/A Vector: N/A	Maybe
Skype for Business 2016 Basic (32-bit)	4475545 Security Update	Important	Information Disclosure	4461473	Base: N/A Temporal:	Maybe

CVE-2019-1084						
					N/A Vector: N/A	
Skype for Business 2016 Basic (64-bit)	4475545 Security Update	Important	Information Disclosure	4461473	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Outlook 2013 Service Pack 1 (32-bit editions)	4464592 Security Update	Important	Information Disclosure	4461595	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Outlook 2013 Service Pack 1 (64-bit editions)	4464592 Security Update	Important	Information Disclosure	4461595	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2019 for 32-bit editions	Click to Run Security Update	Important	Information Disclosure	4461595	Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Office 2019 for 64-bit editions	Click to Run Security Update	Important	Information Disclosure	4461595	Base: N/A Temporal: N/A Vector: N/A	No

CVE-2019-1084						
Microsoft Office 2019 for Mac		Important	Information Disclosure	4461595	Base: N/A Temporal: N/A Vector: N/A	
Office 365 ProPlus for 32-bit Systems	Click to Run Security Update	Important	Information Disclosure	4461595	Base: N/A Temporal: N/A Vector: N/A	No
Office 365 ProPlus for 64-bit Systems	Click to Run Security Update	Important	Information Disclosure	4461595	Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Exchange Server 2016 Cumulative Update 12	4509409 Security Update	Important	Information Disclosure	4503027	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Exchange Server 2019 Cumulative Update 1	4509408 Security Update	Important	Information Disclosure	4503027	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Exchange Server 2019 Cumulative Update 2	4509408 Security Update	Important	Information Disclosure	4503027	Base: N/A Temporal:	Maybe

CVE-2019-1084						
					N/A Vector: N/A	
Microsoft Exchange Server 2016 Cumulative Update 13	4509409 Security Update	Important	Information Disclosure	4503027	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Exchange Server 2013 Cumulative Update 23	4509409 Security Update	Important	Information Disclosure	4503027	Base: N/A Temporal: N/A Vector: N/A	Maybe
Mail and Calendar	Release Notes Security Update	Important	Information Disclosure	4503027	Base: N/A Temporal: N/A Vector: N/A	Maybe
Outlook for iOS		Important	Information Disclosure	4503027	Base: N/A Temporal: N/A Vector: N/A	

CVE-2019-1085 - Windows WLAN Service Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1085 MITRE NVD	**CVE Title:** Windows WLAN Service Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in the way that the wlansvc.dll handles objects in memory. An attacker who successfully exploited the vulnerability could execute code with elevated permissions. To exploit the vulnerability, a locally authenticated attacker could run a specially crafted application. The security update addresses the vulnerability by ensuring the wlansvc.dll properly handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1085						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4507449 Monthly Rollup 4507456 Security Only	Important	Elevation of Privilege	4503292	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-2019-1085						
Windows 7 for x64-based Systems Service Pack 1	4507449 Monthly Rollup 4507456 Security Only	Important	Elevation of Privilege	4503292	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 Core installation)	4507449 Monthly Rollup 4507456 Security Only	Important	Elevation of Privilege	4503292	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	4507449 Monthly Rollup 4507456 Security Only	Important	Elevation of Privilege	4503292	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-2019-1085						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4507449 Monthly Rollup 4507456 Security Only	Important	Elevation of Privilege	4503292	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 Core installation)	4507452 Monthly Rollup 4507461 Security Only	Important	Elevation of Privilege	4503273	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	4507462 Monthly Rollup 4507464 Security Only	Important	Elevation of Privilege	4503285	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-2019-1085						
Windows Server 2012 (Server Core installation)	4507462 Monthly Rollup 4507464 Security Only	Important	Elevation of Privilege	4503285	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	4507448 Monthly Rollup 4507457 Security Only	Important	Elevation of Privilege	4503276	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	4507448 Monthly Rollup 4507457 Security Only	Important	Elevation of Privilege	4503276	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	4507448 Monthly Rollup 4507457 Security	Important	Elevation of Privilege	4503276	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-2019-1085						
	Only					
Windows RT 8.1	4507448 Monthly Rollup	Important	Elevation of Privilege	4503276	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)	4507448 Monthly Rollup 4507457 Security Only	Important	Elevation of Privilege	4503276	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	4507458 Security Update	Important	Elevation of Privilege	4503291	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	4507458 Security Update	Important	Elevation of Privilege	4503291	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	4507460 Security Update	Important	Elevation of Privilege	4503267	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-2019-1085						
Windows 10 Version 1607 for 32-bit Systems	4507460 Security Update	Important	Elevation of Privilege	4503267	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	4507460 Security Update	Important	Elevation of Privilege	4503267	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)	4507460 Security Update	Important	Elevation of Privilege	4503267	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	4507450 Security Update	Important	Elevation of Privilege	4503279	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	4507450 Security Update	Important	Elevation of Privilege	4503279	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-2019-1085						
Windows 10 Version 1709 for 32-bit Systems	4507455 Security Update	Important	Elevation of Privilege	4503284	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	4507455 Security Update	Important	Elevation of Privilege	4503284	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	4507435 Security Update	Important	Elevation of Privilege	4503286	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	4507435 Security Update	Important	Elevation of Privilege	4503286	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	4507435 Security Update	Important	Elevation of Privilege	4503286	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-2019-1085						
Core Installation)						
Windows 10 Version 1803 for ARM64-based Systems	4507435 Security Update	Important	Elevation of Privilege	4503286	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	4507469 Security Update	Important	Elevation of Privilege	4503327	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	4507469 Security Update	Important	Elevation of Privilege	4503327	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	4507469 Security Update	Important	Elevation of Privilege	4503327	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-2019-1085						
Windows Server 2019	4507469 Security Update	Important	Elevation of Privilege	4503327	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)	4507469 Security Update	Important	Elevation of Privilege	4503327	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	4507455 Security Update	Important	Elevation of Privilege	4503284	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	4507453 Security Update	Important	Elevation of Privilege	4503293	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	4507453 Security Update	Important	Elevation of Privilege	4503293	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-2019-1085						
Windows 10 Version 1903 for ARM64-based Systems	4507453 Security Update	Important	Elevation of Privilege	4503293	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)	4507453 Security Update	Important	Elevation of Privilege	4503293	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	4507452 Monthly Rollup 4507461 Security Only	Important	Elevation of Privilege	4503273	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	4507452 Monthly Rollup 4507461	Important	Elevation of Privilege	4503273	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-2019-1085						
Service Pack 2	Security Only					
Windows Server 2008 for x64-based Systems Service Pack 2	4507452 Monthly Rollup 4507461 Security Only	Important	Elevation of Privilege	4503273	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)	4507452 Monthly Rollup 4507461 Security Only	Important	Elevation of Privilege	4503273	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-2019-1086 - Windows Audio Service Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1086 MITRE NVD	**CVE Title:** Windows Audio Service Elevation of Privilege Vulnerability **Description:** An elevation of privilege exists in Windows Audio Service. An attacker who successfully exploited the vulnerability could run arbitrary code with elevated privileges. To exploit the vulnerability, an attacker could run a specially crafted application that could exploit the vulnerability. This vulnerability by itself does not allow arbitrary code to be run. However, this vulnerability could be used in conjunction with one or more vulnerabilities (e.g. a remote code execution vulnerability and another elevation of privilege) that could take advantage of the elevated privileges when running. The update addresses the vulnerability by correcting how the Windows Audio Service handles processes these requests. **FAQ:** None	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1086						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 8.1 for 32-bit systems	4507448 Monthly Rollup 4507457	Important	Elevation of Privilege	4503276	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-2019-1086						
	Security Only					
Windows 8.1 for x64-based systems	4507448 Monthly Rollup 4507457 Security Only	Important	Elevation of Privilege	4503276	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	4507448 Monthly Rollup 4507457 Security Only	Important	Elevation of Privilege	4503276	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	4507448 Monthly Rollup	Important	Elevation of Privilege	4503276	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)	4507448 Monthly Rollup 4507457 Security	Important	Elevation of Privilege	4503276	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-2019-1086						
	Only					
Windows 10 for 32-bit Systems	4507458 Security Update	Important	Elevation of Privilege	4503291	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	4507458 Security Update	Important	Elevation of Privilege	4503291	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	4507460 Security Update	Important	Elevation of Privilege	4503267	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	4507460 Security Update	Important	Elevation of Privilege	4503267	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	4507460 Security Update	Important	Elevation of Privilege	4503267	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-2019-1086						
Windows Server 2016 (Server Core installation)	4507460 Security Update	Important	Elevation of Privilege	4503267	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	4507450 Security Update	Important	Elevation of Privilege	4503279	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	4507450 Security Update	Important	Elevation of Privilege	4503279	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	4507455 Security Update	Important	Elevation of Privilege	4503284	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	4507455 Security Update	Important	Elevation of Privilege	4503284	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-2019-1086						
Windows 10 Version 1803 for 32-bit Systems	4507435 Security Update	Important	Elevation of Privilege	4503286	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	4507435 Security Update	Important	Elevation of Privilege	4503286	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)	4507435 Security Update	Important	Elevation of Privilege	4503286	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	4507435 Security Update	Important	Elevation of Privilege	4503286	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-2019-1086						
Windows 10 Version 1809 for 32-bit Systems	4507469 Security Update	Important	Elevation of Privilege	4503327	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	4507469 Security Update	Important	Elevation of Privilege	4503327	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	4507469 Security Update	Important	Elevation of Privilege	4503327	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	4507469 Security Update	Important	Elevation of Privilege	4503327	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)	4507469 Security Update	Important	Elevation of Privilege	4503327	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-2019-1086						
Windows 10 Version 1709 for ARM64-based Systems	4507455 Security Update	Important	Elevation of Privilege	4503284	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	4507453 Security Update	Important	Elevation of Privilege	4503293	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	4507453 Security Update	Important	Elevation of Privilege	4503293	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	4507453 Security Update	Important	Elevation of Privilege	4503293	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-2019-1086						
Windows Server, version 1903 (Server Core installation)	4507453 Security Update	Important	Elevation of Privilege	4503293	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-2019-1087 - Windows Audio Service Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1087 MITRE NVD	**CVE Title:** Windows Audio Service Elevation of Privilege Vulnerability **Description:** An elevation of privilege exists in Windows Audio Service. An attacker who successfully exploited the vulnerability could run arbitrary code with elevated privileges. To exploit the vulnerability, an attacker could run a specially crafted application that could exploit the vulnerability. This vulnerability by itself does not allow arbitrary code to be run. However, this vulnerability could be used in conjunction with one or more	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	vulnerabilities (e.g. a remote code execution vulnerability and another elevation of privilege) that could take advantage of the elevated privileges when running. The update addresses the vulnerability by correcting how the Windows Audio Service handles processes these requests. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1087						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 8.1 for 32-bit systems	4507448 Monthly Rollup 4507457 Security Only	Important	Elevation of Privilege	4503276	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	4507448 Monthly Rollup 4507457 Security Only	Important	Elevation of Privilege	4503276	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	4507448 Monthly Rollup 4507457 Security Only	Important	Elevation of Privilege	4503276	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	4507448 Monthly Rollup	Important	Elevation of Privilege	4503276	Base: 7.8 Temporal: 7	Yes

CVE-2019-1087						
					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 2012 R2 (Server Core installation)	4507448 Monthly Rollup 4507457 Security Only	Important	Elevation of Privilege	4503276	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	4507458 Security Update	Important	Elevation of Privilege	4503291	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	4507458 Security Update	Important	Elevation of Privilege	4503291	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	4507460 Security Update	Important	Elevation of Privilege	4503267	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	4507460 Security Update	Important	Elevation of Privilege	4503267	Base: 7.8 Temporal: 7	Yes

CVE-2019-1087						
1607 for 32-bit Systems					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 1607 for x64-based Systems	4507460 Security Update	Important	Elevation of Privilege	4503267	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)	4507460 Security Update	Important	Elevation of Privilege	4503267	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	4507450 Security Update	Important	Elevation of Privilege	4503279	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	4507450 Security Update	Important	Elevation of Privilege	4503279	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	4507455 Security Update	Important	Elevation of Privilege	4503284	Base: 7.8 Temporal: 7	Yes

CVE-2019-1087						
1709 for 32-bit Systems					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 1709 for x64-based Systems	4507455 Security Update	Important	Elevation of Privilege	4503284	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	4507435 Security Update	Important	Elevation of Privilege	4503286	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	4507435 Security Update	Important	Elevation of Privilege	4503286	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)	4507435 Security Update	Important	Elevation of Privilege	4503286	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-2019-1087						
Windows 10 Version 1803 for ARM64-based Systems	4507435 Security Update	Important	Elevation of Privilege	4503286	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	4507469 Security Update	Important	Elevation of Privilege	4503327	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	4507469 Security Update	Important	Elevation of Privilege	4503327	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	4507469 Security Update	Important	Elevation of Privilege	4503327	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-2019-1087						
Windows Server 2019	4507469 Security Update	Important	Elevation of Privilege	4503327	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)	4507469 Security Update	Important	Elevation of Privilege	4503327	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	4507455 Security Update	Important	Elevation of Privilege	4503284	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	4507453 Security Update	Important	Elevation of Privilege	4503293	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	4507453 Security Update	Important	Elevation of Privilege	4503293	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-2019-1087						
Windows 10 Version 1903 for ARM64-based Systems	4507453 Security Update	Important	Elevation of Privilege	4503293	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)	4507453 Security Update	Important	Elevation of Privilege	4503293	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-2019-1088 - Windows Audio Service Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1088 MITRE NVD	**CVE Title:** Windows Audio Service Elevation of Privilege Vulnerability **Description:** An elevation of privilege exists in Windows Audio Service. An attacker who successfully exploited the vulnerability could run arbitrary code with elevated privileges. To exploit the vulnerability, an attacker could run a specially crafted application that could exploit the vulnerability. This vulnerability by itself does not allow arbitrary code to be run. However, this vulnerability could be used in conjunction with one or more vulnerabilities (e.g. a remote code execution vulnerability and another elevation of privilege) that could take advantage of the elevated privileges when running. The update addresses the vulnerability by correcting how the Windows Audio Service handles processes these requests. **FAQ:** None	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1088						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems	4507449 Monthly Rollup 4507456	Important	Elevation of Privilege	4503292	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-2019-1088						
Service Pack 1	Security Only					
Windows 7 for x64-based Systems Service Pack 1	4507449 Monthly Rollup 4507456 Security Only	Important	Elevation of Privilege	4503292	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 Core installation)	4507449 Monthly Rollup 4507456 Security Only	Important	Elevation of Privilege	4503292	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	4507449 Monthly Rollup 4507456 Security Only	Important	Elevation of Privilege	4503292	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-2019-1088						
Service Pack 1						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4507449 Monthly Rollup 4507456 Security Only	Important	Elevation of Privilege	4503292	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 Core installation)	4507452 Monthly Rollup 4507461 Security Only	Important	Elevation of Privilege	4503273	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	4507462 Monthly Rollup 4507464 Security Only	Important	Elevation of Privilege	4503285	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-2019-1088						
Windows Server 2012 (Server Core installation)	4507462 Monthly Rollup 4507464 Security Only	Important	Elevation of Privilege	4503285	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	4507448 Monthly Rollup 4507457 Security Only	Important	Elevation of Privilege	4503276	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	4507448 Monthly Rollup 4507457 Security Only	Important	Elevation of Privilege	4503276	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	4507448 Monthly Rollup 4507457 Security	Important	Elevation of Privilege	4503276	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-2019-1088						
	Only					
Windows RT 8.1	4507448 Monthly Rollup	Important	Elevation of Privilege	4503276	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)	4507448 Monthly Rollup 4507457 Security Only	Important	Elevation of Privilege	4503276	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	4507458 Security Update	Important	Elevation of Privilege	4503291	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	4507458 Security Update	Important	Elevation of Privilege	4503291	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	4507460 Security Update	Important	Elevation of Privilege	4503267	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-2019-1088						
Windows 10 Version 1607 for 32-bit Systems	4507460 Security Update	Important	Elevation of Privilege	4503267	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	4507460 Security Update	Important	Elevation of Privilege	4503267	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)	4507460 Security Update	Important	Elevation of Privilege	4503267	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	4507450 Security Update	Important	Elevation of Privilege	4503279	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	4507450 Security Update	Important	Elevation of Privilege	4503279	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-2019-1088						
Windows 10 Version 1709 for 32-bit Systems	4507455 Security Update	Important	Elevation of Privilege	4503284	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	4507455 Security Update	Important	Elevation of Privilege	4503284	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	4507435 Security Update	Important	Elevation of Privilege	4503286	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	4507435 Security Update	Important	Elevation of Privilege	4503286	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	4507435 Security Update	Important	Elevation of Privilege	4503286	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-2019-1088						
Core Installation)						
Windows 10 Version 1803 for ARM64-based Systems	4507435 Security Update	Important	Elevation of Privilege	4503286	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	4507469 Security Update	Important	Elevation of Privilege	4503327	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	4507469 Security Update	Important	Elevation of Privilege	4503327	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	4507469 Security Update	Important	Elevation of Privilege	4503327	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-2019-1088						
Windows Server 2019	4507469 Security Update	Important	Elevation of Privilege	4503327	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)	4507469 Security Update	Important	Elevation of Privilege	4503327	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	4507455 Security Update	Important	Elevation of Privilege	4503284	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	4507453 Security Update	Important	Elevation of Privilege	4503293	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	4507453 Security Update	Important	Elevation of Privilege	4503293	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-2019-1088						
Windows 10 Version 1903 for ARM64-based Systems	4507453 Security Update	Important	Elevation of Privilege	4503293	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)	4507453 Security Update	Important	Elevation of Privilege	4503293	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	4507452 Monthly Rollup 4507461 Security Only	Important	Elevation of Privilege	4503273	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	4507452 Monthly Rollup 4507461	Important	Elevation of Privilege	4503273	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-2019-1088						
Service Pack 2	Security Only					
Windows Server 2008 for x64-based Systems Service Pack 2	4507452 Monthly Rollup 4507461 Security Only	Important	Elevation of Privilege	4503273	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)	4507452 Monthly Rollup 4507461 Security Only	Important	Elevation of Privilege	4503273	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-2019-1089 - Windows RPCSS Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1089 MITRE NVD	**CVE Title:** Windows RPCSS Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in rpcss.dll when the RPC service Activation Kernel improperly handles an RPC request. To exploit this vulnerability, a low level authenticated attacker could run a specially crafted application. The security update addresses this vulnerability by correcting how rpcss.dll handles these requests. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 07/09/2019 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-2019-1089						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4507449 Monthly Rollup 4507456 Security Only	Important	Elevation of Privilege	4503292	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	4507449 Monthly Rollup 4507456 Security	Important	Elevation of Privilege	4503292	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-2019-1089						
Service Pack 1	Only					
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4507449 Monthly Rollup 4507456 Security Only	Important	Elevation of Privilege	4503292	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	4507449 Monthly Rollup 4507456 Security Only	Important	Elevation of Privilege	4503292	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	4507449 Monthly Rollup 4507456	Important	Elevation of Privilege	4503292	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-2019-1089						
Systems Service Pack 1	Security Only					
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4507452 Monthly Rollup 4507461 Security Only	Important	Elevation of Privilege	4503273	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	4507462 Monthly Rollup 4507464 Security Only	Important	Elevation of Privilege	4503285	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)	4507462 Monthly Rollup 4507464 Security Only	Important	Elevation of Privilege	4503285	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-2019-1089						
Windows 8.1 for 32-bit systems	4507448 Monthly Rollup 4507457 Security Only	Important	Elevation of Privilege	4503276	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	4507448 Monthly Rollup 4507457 Security Only	Important	Elevation of Privilege	4503276	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	4507448 Monthly Rollup 4507457 Security Only	Important	Elevation of Privilege	4503276	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	4507448 Monthly Rollup	Important	Elevation of Privilege	4503276	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-2019-1089						
Windows Server 2012 R2 (Server Core installation)	4507448 Monthly Rollup 4507457 Security Only	Important	Elevation of Privilege	4503276	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	4507458 Security Update	Important	Elevation of Privilege	4503291	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	4507458 Security Update	Important	Elevation of Privilege	4503291	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	4507460 Security Update	Important	Elevation of Privilege	4503267	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	4507460 Security Update	Important	Elevation of Privilege	4503267	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-2019-1089						
Windows 10 Version 1607 for x64-based Systems	4507460 Security Update	Important	Elevation of Privilege	4503267	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)	4507460 Security Update	Important	Elevation of Privilege	4503267	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	4507450 Security Update	Important	Elevation of Privilege	4503279	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	4507450 Security Update	Important	Elevation of Privilege	4503279	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	4507455 Security Update	Important	Elevation of Privilege	4503284	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-2019-1089						
Windows 10 Version 1709 for x64-based Systems	4507455 Security Update	Important	Elevation of Privilege	4503284	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	4507435 Security Update	Important	Elevation of Privilege	4503286	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	4507435 Security Update	Important	Elevation of Privilege	4503286	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)	4507435 Security Update	Important	Elevation of Privilege	4503286	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	4507435 Security Update	Important	Elevation of Privilege	4503286	Base: 7.8 Temporal: 7	Yes

CVE-2019-1089						
ARM64-based Systems					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 1809 for 32-bit Systems	4507469 Security Update	Important	Elevation of Privilege	4503327	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	4507469 Security Update	Important	Elevation of Privilege	4503327	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	4507469 Security Update	Important	Elevation of Privilege	4503327	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	4507469 Security Update	Important	Elevation of Privilege	4503327	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-2019-1089						
Windows Server 2019 (Server Core installation)	4507469 Security Update	Important	Elevation of Privilege	4503327	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	4507455 Security Update	Important	Elevation of Privilege	4503284	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	4507453 Security Update	Important	Elevation of Privilege	4503293	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	4507453 Security Update	Important	Elevation of Privilege	4503293	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-	4507453 Security Update	Important	Elevation of Privilege	4503293	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-2019-1089						
based Systems						
Windows Server, version 1903 (Server Core installation)	4507453 Security Update	Important	Elevation of Privilege	4503293	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	4507452 Monthly Rollup 4507461 Security Only	Important	Elevation of Privilege	4503273	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	4507452 Monthly Rollup 4507461 Security Only	Important	Elevation of Privilege	4503273	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-2019-1089						
Windows Server 2008 for x64-based Systems Service Pack 2	4507452 Monthly Rollup 4507461 Security Only	Important	Elevation of Privilege	4503273	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)	4507452 Monthly Rollup 4507461 Security Only	Important	Elevation of Privilege	4503273	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-2019-1090 - Windows dnsrlvr.dll Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1090 MITRE NVD	**CVE Title:** Windows dnsrlvr.dll Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in the way that the dnsrslvr.dll handles objects in memory. An attacker who successfully exploited the vulnerability could execute code with elevated permissions. To exploit the vulnerability, a locally authenticated attacker could run a specially crafted application. The security update addresses the vulnerability by ensuring the dnsrslvr.dll properly handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 07/09/2019 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-2019-1090						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4507435 Security Update	Important	Elevation of Privilege	4503286	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	4507435 Security Update	Important	Elevation of Privilege	4503286	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-2019-1090						
Windows Server, version 1803 (Server Core Installation)	4507435 Security Update	Important	Elevation of Privilege	4503286	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	4507435 Security Update	Important	Elevation of Privilege	4503286	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	4507469 Security Update	Important	Elevation of Privilege	4503327	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	4507469 Security Update	Important	Elevation of Privilege	4503327	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-2019-1090						
Windows 10 Version 1809 for ARM64-based Systems	4507469 Security Update	Important	Elevation of Privilege	4503327	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	4507469 Security Update	Important	Elevation of Privilege	4503327	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)	4507469 Security Update	Important	Elevation of Privilege	4503327	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	4507453 Security Update	Important	Elevation of Privilege	4503293	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	4507453 Security Update	Important	Elevation of Privilege	4503293	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-2019-1090						
Windows 10 Version 1903 for ARM64-based Systems	4507453 Security Update	Important	Elevation of Privilege	4503293	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)	4507453 Security Update	Important	Elevation of Privilege	4503293	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-2019-1091 - Microsoft unistore.dll Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-	**CVE Title:** Microsoft unistore.dll Information Disclosure Vulnerability **Description:**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
1091 MITRE NVD	An information disclosure vulnerability exists when Unistore.dll 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 Unistore.dll 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 server object address. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 07/09/2019 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-2019-1091						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	4507458 Security Update	Important	Information Disclosure	4503291	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	4507458 Security Update	Important	Information Disclosure	4503291	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-2019-1091						
Windows Server 2016	4507460 Security Update	Important	Information Disclosure	4503267	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 32-bit Systems	4507460 Security Update	Important	Information Disclosure	4503267	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	4507460 Security Update	Important	Information Disclosure	4503267	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)	4507460 Security Update	Important	Information Disclosure	4503267	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	4507450 Security	Important	Information Disclosure	4503279	Base: 5.5 Temporal: 5	Yes

CVE-2019-1091						
1703 for 32-bit 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 1703 for x64-based Systems	4507450 Security Update	Important	Information Disclosure	4503279	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 32-bit Systems	4507455 Security Update	Important	Information Disclosure	4503284	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	4507455 Security Update	Important	Information Disclosure	4503284	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	4507435 Security Update	Important	Information Disclosure	4503286	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-2019-1091						
Windows 10 Version 1803 for x64-based Systems	4507435 Security Update	Important	Information Disclosure	4503286	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 1803 (Server Core Installation)	4507435 Security Update	Important	Information Disclosure	4503286	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	4507435 Security Update	Important	Information Disclosure	4503286	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	4507469 Security Update	Important	Information Disclosure	4503327	Base: 5.5 Temporal: 5 Vector:	Yes

CVE-2019-1091						
32-bit 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 x64-based Systems	4507469 Security Update	Important	Information Disclosure	4503327	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	4507469 Security Update	Important	Information Disclosure	4503327	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	4507469 Security Update	Important	Information Disclosure	4503327	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	4507469 Security Update	Important	Information Disclosure	4503327	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-2019-1091						
Core installation)						
Windows 10 Version 1709 for ARM64-based Systems	4507455 Security Update	Important	Information Disclosure	4503284	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	4507453 Security Update	Important	Information Disclosure	4503293	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	4507453 Security Update	Important	Information Disclosure	4503293	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-	4507453 Security Update	Important	Information Disclosure	4503293	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-2019-1091						
based Systems						
Windows Server, version 1903 (Server Core installation)	4507453 Security Update	Important	Information Disclosure	4503293	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-2019-1092 - Chakra Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1092	**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	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	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 **Workarounds:** None		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1092						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4507458 Security Update	Critical	Remote Code Execution	4503291	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 on Windows	4507458 Security Update	Critical	Remote Code Execution	4503291	Base: 4.2 Temporal: 3.8	Yes

CVE-2019-1092						
10 for x64-based Systems					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 on Windows Server 2016	4507460 Security Update	Moderate	Remote Code Execution	4503267	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 on Windows 10 Version 1607 for 32-bit Systems	4507460 Security Update	Critical	Remote Code Execution	4503267	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 on Windows 10 Version 1607 for x64-based Systems	4507460 Security Update	Critical	Remote Code Execution	4503267	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-2019-1092						
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4507450 Security Update	Critical	Remote Code Execution	4503279	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 on Windows 10 Version 1703 for x64-based Systems	4507450 Security Update	Critical	Remote Code Execution	4503279	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 on Windows 10 Version 1709 for 32-bit Systems	4507455 Security Update	Critical	Remote Code Execution	4503284	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-2019-1092						
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4507455 Security Update	Critical	Remote Code Execution	4503284	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 on Windows 10 Version 1803 for 32-bit Systems	4507435 Security Update	Critical	Remote Code Execution	4503286	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 on Windows 10 Version 1803 for x64-based Systems	4507435 Security Update	Critical	Remote Code Execution	4503286	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-2019-1092						
Microsoft Edge on Windows 10 Version 1803 for ARM64-based Systems	4507435 Security Update	Critical	Remote Code Execution	4503286	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 on Windows 10 Version 1809 for 32-bit Systems	4507469 Security Update	Critical	Remote Code Execution	4503327	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 on Windows 10 Version 1809 for x64-based Systems	4507469 Security Update	Critical	Remote Code Execution	4503327	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-2019-1092						
Microsoft Edge on Windows 10 Version 1809 for ARM64-based Systems	4507469 Security Update	Critical	Remote Code Execution	4503327	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 on Windows Server 2019	4507469 Security Update	Moderate	Remote Code Execution	4503327	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 on Windows 10 Version 1709 for ARM64-based Systems	4507455 Security Update	Critical	Remote Code Execution	4503284	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 on Windows	4507453 Security Update	Critical	Remote Code Execution	4503293	Base: 4.2 Temporal: 3.8	Yes

CVE-2019-1092						
10 Version 1903 for 32-bit Systems					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 on Windows 10 Version 1903 for x64-based Systems	4507453 Security Update	Critical	Remote Code Execution	4503293	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 on Windows 10 Version 1903 for ARM64-based Systems	4507453 Security Update	Critical	Remote Code Execution	4503293	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	4503293	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-2019-1093 - DirectWrite Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1093 MITRE NVD	**CVE Title:** DirectWrite Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when DirectWrite improperly discloses the contents of its memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system. There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document, or by convincing a user to visit an untrusted webpage. The security update addresses the vulnerability by correcting how DirectWrite 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 memory layout - the vulnerability allows an attacker to collect information that facilitates predicting addressing of the memory.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1093						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit	4507449 Monthly	Important	Information Disclosure	4503292	Base: 5.5 Temporal: 5	Yes

CVE-2019-1093						
Systems Service Pack 1	Rollup 4507456 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 7 for x64-based Systems Service Pack 1	4507449 Monthly Rollup 4507456 Security Only	Important	Information Disclosure	4503292	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 Core installation)	4507449 Monthly Rollup 4507456 Security Only	Important	Information Disclosure	4503292	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	4507449 Monthly Rollup	Important	Information Disclosure	4503292	Base: 5.5 Temporal: 5 Vector:	Yes

CVE-2019-1093						
Itanium-Based Systems Service Pack 1	4507456 Security Only				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 x64-based Systems Service Pack 1	4507449 Monthly Rollup 4507456 Security Only	Important	Information Disclosure	4503292	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 (Server Core installation)	4507452 Monthly Rollup 4507461 Security Only	Important	Information Disclosure	4503273	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-2019-1093						
Windows Server 2012	4507462 Monthly Rollup 4507464 Security Only	Important	Information Disclosure	4503285	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)	4507462 Monthly Rollup 4507464 Security Only	Important	Information Disclosure	4503285	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	4507448 Monthly Rollup 4507457 Security Only	Important	Information Disclosure	4503276	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 x64-based systems	4507448 Monthly Rollup 4507457 Security	Important	Information Disclosure	4503276	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-2019-1093						
	Only					
Windows Server 2012 R2	4507448 Monthly Rollup 4507457 Security Only	Important	Information Disclosure	4503276	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	4507448 Monthly Rollup	Important	Information Disclosure	4503276	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 (Server Core installation)	4507448 Monthly Rollup 4507457 Security Only	Important	Information Disclosure	4503276	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	4507458 Security Update	Important	Information Disclosure	4503291	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-2019-1093						
Windows 10 for x64-based Systems	4507458 Security Update	Important	Information Disclosure	4503291	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	4507460 Security Update	Important	Information Disclosure	4503267	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 32-bit Systems	4507460 Security Update	Important	Information Disclosure	4503267	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	4507460 Security Update	Important	Information Disclosure	4503267	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	4507460 Security Update	Important	Information Disclosure	4503267	Base: 5.5 Temporal: 5 Vector:	Yes

CVE-2019-1093						
(Server Core installation)					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 1703 for 32-bit Systems	4507450 Security Update	Important	Information Disclosure	4503279	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 x64-based Systems	4507450 Security Update	Important	Information Disclosure	4503279	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 32-bit Systems	4507455 Security Update	Important	Information Disclosure	4503284	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	4507455 Security Update	Important	Information Disclosure	4503284	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-2019-1093						
Windows 10 Version 1803 for 32-bit Systems	4507435 Security Update	Important	Information Disclosure	4503286	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	4507435 Security Update	Important	Information Disclosure	4503286	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 1803 (Server Core Installation)	4507435 Security Update	Important	Information Disclosure	4503286	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-	4507435 Security Update	Important	Information Disclosure	4503286	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-2019-1093						
based Systems						
Windows 10 Version 1809 for 32-bit Systems	4507469 Security Update	Important	Information Disclosure	4503327	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	4507469 Security Update	Important	Information Disclosure	4503327	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	4507469 Security Update	Important	Information Disclosure	4503327	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	4507469 Security Update	Important	Information Disclosure	4503327	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-2019-1093						
Windows Server 2019 (Server Core installation)	4507469 Security Update	Important	Information Disclosure	4503327	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-based Systems	4507455 Security Update	Important	Information Disclosure	4503284	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	4507453 Security Update	Important	Information Disclosure	4503293	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	4507453 Security Update	Important	Information Disclosure	4503293	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-2019-1093						
Windows 10 Version 1903 for ARM64-based Systems	4507453 Security Update	Important	Information Disclosure	4503293	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 Core installation)	4507453 Security Update	Important	Information Disclosure	4503293	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 Itanium-Based Systems Service Pack 2	4507452 Monthly Rollup 4507461 Security Only	Important	Information Disclosure	4503273	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	4507452 Monthly	Important	Information Disclosure	4503273	Base: 5.5 Temporal: 5	Yes

CVE-2019-1093						
2008 for 32-bit Systems Service Pack 2	Rollup 4507461 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 for x64-based Systems Service Pack 2	4507452 Monthly Rollup 4507461 Security Only	Important	Information Disclosure	4503273	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 Service Pack 2 (Server Core installation)	4507452 Monthly Rollup 4507461 Security Only	Important	Information Disclosure	4503273	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-2019-1094 - Windows GDI Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1094 MITRE NVD	**CVE Title:** Windows GDI Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system. There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document, or by convincing a user to visit an untrusted webpage. The security update addresses the vulnerability by correcting how the Windows GDI component 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 memory layout - the vulnerability allows an attacker to collect information that facilitates predicting addressing of the memory. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1094						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4507449 Monthly Rollup 4507456 Security Only	Important	Information Disclosure	4503292	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	4507449 Monthly Rollup 4507456 Security Only	Important	Information Disclosure	4503292	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	4507449 Monthly Rollup 4507456 Security Only	Important	Information Disclosure	4503292	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-2019-1094						
Core installation)						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4507449 Monthly Rollup 4507456 Security Only	Important	Information Disclosure	4503292	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	4507449 Monthly Rollup 4507456 Security Only	Important	Information Disclosure	4503292	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	4507452 Monthly Rollup 4507461 Security Only	Important	Information Disclosure	4503273	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-2019-1094						
Pack 2 (Server Core installation)						
Windows Server 2012	4507462 Monthly Rollup 4507464 Security Only	Important	Information Disclosure	4503285	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)	4507462 Monthly Rollup 4507464 Security Only	Important	Information Disclosure	4503285	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	4507448 Monthly Rollup 4507457 Security Only	Important	Information Disclosure	4503276	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-2019-1094						
Windows 8.1 for x64-based systems	4507448 Monthly Rollup 4507457 Security Only	Important	Information Disclosure	4503276	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	4507448 Monthly Rollup 4507457 Security Only	Important	Information Disclosure	4503276	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	4507448 Monthly Rollup	Important	Information Disclosure	4503276	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 (Server Core installation)	4507448 Monthly Rollup 4507457 Security Only	Important	Information Disclosure	4503276	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-2019-1094						
Windows 10 for 32-bit Systems	4507458 Security Update	Important	Information Disclosure	4503291	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	4507458 Security Update	Important	Information Disclosure	4503291	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	4507460 Security Update	Important	Information Disclosure	4503267	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 32-bit Systems	4507460 Security Update	Important	Information Disclosure	4503267	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	4507460 Security Update	Important	Information Disclosure	4503267	Base: 5.5 Temporal: 5 Vector:	Yes

CVE-2019-1094						
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 Server 2016 (Server Core installation)	4507460 Security Update	Important	Information Disclosure	4503267	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	4507450 Security Update	Important	Information Disclosure	4503279	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 x64-based Systems	4507450 Security Update	Important	Information Disclosure	4503279	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 32-bit Systems	4507455 Security Update	Important	Information Disclosure	4503284	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-2019-1094						
Windows 10 Version 1709 for x64-based Systems	4507455 Security Update	Important	Information Disclosure	4503284	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	4507435 Security Update	Important	Information Disclosure	4503286	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	4507435 Security Update	Important	Information Disclosure	4503286	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 1803 (Server Core Installation)	4507435 Security Update	Important	Information Disclosure	4503286	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-2019-1094						
Windows 10 Version 1803 for ARM64-based Systems	4507435 Security Update	Important	Information Disclosure	4503286	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	4507469 Security Update	Important	Information Disclosure	4503327	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	4507469 Security Update	Important	Information Disclosure	4503327	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	4507469 Security Update	Important	Information Disclosure	4503327	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-2019-1094						
Windows Server 2019	4507469 Security Update	Important	Information Disclosure	4503327	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)	4507469 Security Update	Important	Information Disclosure	4503327	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-based Systems	4507455 Security Update	Important	Information Disclosure	4503284	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	4507453 Security Update	Important	Information Disclosure	4503293	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-2019-1094						
Windows 10 Version 1903 for x64-based Systems	4507453 Security Update	Important	Information Disclosure	4503293	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	4507453 Security Update	Important	Information Disclosure	4503293	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 Core installation)	4507453 Security Update	Important	Information Disclosure	4503293	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 Itanium-Based	4507452 Monthly Rollup 4507461 Security	Important	Information Disclosure	4503273	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-2019-1094						
Systems Service Pack 2	Only					
Windows Server 2008 for 32-bit Systems Service Pack 2	4507452 Monthly Rollup 4507461 Security Only	Important	Information Disclosure	4503273	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 Service Pack 2	4507452 Monthly Rollup 4507461 Security Only	Important	Information Disclosure	4503273	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 Service	4507452 Monthly Rollup 4507461 Security Only	Important	Information Disclosure	4503273	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-2019-1094						
Pack 2 (Server Core installation)						

CVE-2019-1095 - Windows GDI Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1095 MITRE NVD	**CVE Title:** Windows GDI Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system. There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document, or by convincing a user to visit an untrusted webpage.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by correcting how the Windows GDI component 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 memory layout - the vulnerability allows an attacker to collect information that facilitates predicting addressing of the memory. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1095						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4507449 Monthly Rollup 4507456 Security Only	Important	Information Disclosure	4503292	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	4507449 Monthly Rollup 4507456 Security Only	Important	Information Disclosure	4503292	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	4507449 Monthly Rollup 4507456	Important	Information Disclosure	4503292	Base: 5.5 Temporal: 5 Vector:	Yes

CVE-2019-1095						
Systems Service Pack 1 (Server Core installation)	Security Only				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	4507449 Monthly Rollup 4507456 Security Only	Important	Information Disclosure	4503292	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	4507449 Monthly Rollup 4507456 Security Only	Important	Information Disclosure	4503292	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	4507452 Monthly	Important	Information Disclosure	4503273	Base: 5.5 Temporal: 5	Yes

CVE-2019-1095						
2008 for 32-bit Systems Service Pack 2 (Server Core installation)	Rollup 4507461 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 2012	4507462 Monthly Rollup 4507464 Security Only	Important	Information Disclosure	4503285	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)	4507462 Monthly Rollup 4507464 Security Only	Important	Information Disclosure	4503285	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	4507448 Monthly Rollup	Important	Information Disclosure	4503276	Base: 5.5 Temporal: 5 Vector:	Yes

CVE-2019-1095						
	4507457 Security Only				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	4507448 Monthly Rollup 4507457 Security Only	Important	Information Disclosure	4503276	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	4507448 Monthly Rollup 4507457 Security Only	Important	Information Disclosure	4503276	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	4507448 Monthly Rollup	Important	Information Disclosure	4503276	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	4507448 Monthly Rollup	Important	Information Disclosure	4503276	Base: 5.5 Temporal: 5 Vector:	Yes

CVE-2019-1095						
(Server Core installation)	4507457 Security Only				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 for 32-bit Systems	4507458 Security Update	Important	Information Disclosure	4503291	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	4507458 Security Update	Important	Information Disclosure	4503291	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	4507460 Security Update	Important	Information Disclosure	4503267	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 32-bit Systems	4507460 Security Update	Important	Information Disclosure	4503267	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-2019-1095						
Windows 10 Version 1607 for x64-based Systems	4507460 Security Update	Important	Information Disclosure	4503267	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)	4507460 Security Update	Important	Information Disclosure	4503267	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	4507450 Security Update	Important	Information Disclosure	4503279	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 x64-based Systems	4507450 Security Update	Important	Information Disclosure	4503279	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	4507455 Security	Important	Information Disclosure	4503284	Base: 5.5 Temporal: 5	Yes

CVE-2019-1095						
1709 for 32-bit 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 x64-based Systems	4507455 Security Update	Important	Information Disclosure	4503284	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	4507435 Security Update	Important	Information Disclosure	4503286	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	4507435 Security Update	Important	Information Disclosure	4503286	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 1803 (Server	4507435 Security Update	Important	Information Disclosure	4503286	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-2019-1095						
Core Installation)						
Windows 10 Version 1803 for ARM64-based Systems	4507435 Security Update	Important	Information Disclosure	4503286	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	4507469 Security Update	Important	Information Disclosure	4503327	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	4507469 Security Update	Important	Information Disclosure	4503327	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-	4507469 Security Update	Important	Information Disclosure	4503327	Base: 5.5 Temporal: 5 Vector:	Yes

CVE-2019-1095						
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 Server 2019	4507469 Security Update	Important	Information Disclosure	4503327	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)	4507469 Security Update	Important	Information Disclosure	4503327	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-based Systems	4507455 Security Update	Important	Information Disclosure	4503284	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	4507453 Security Update	Important	Information Disclosure	4503293	Base: 5.5 Temporal: 5 Vector:	Yes

CVE-2019-1095						
32-bit 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 x64-based Systems	4507453 Security Update	Important	Information Disclosure	4503293	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	4507453 Security Update	Important	Information Disclosure	4503293	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 Core installation)	4507453 Security Update	Important	Information Disclosure	4503293	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	4507452 Monthly Rollup	Important	Information Disclosure	4503273	Base: 5.5 Temporal: 5 Vector:	Yes

CVE-2019-1095						
Itanium-Based Systems Service Pack 2	4507461 Security Only				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 for 32-bit Systems Service Pack 2	4507452 Monthly Rollup 4507461 Security Only	Important	Information Disclosure	4503273	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 Service Pack 2	4507452 Monthly Rollup 4507461 Security Only	Important	Information Disclosure	4503273	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	4507452 Monthly Rollup 4507461	Important	Information Disclosure	4503273	Base: 5.5 Temporal: 5 Vector:	Yes

CVE-2019-1095						
Systems Service Pack 2 (Server Core installation)	Security Only				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	

CVE-2019-1096 - Win32k Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1096 MITRE NVD	**CVE Title:** Win32k Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the win32k component improperly provides kernel information. An attacker who successfully exploited the 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.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by correcting how win32k 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 memory layout - the vulnerability allows an attacker to collect information that facilitates predicting addressing of the memory. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1096						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4507449 Monthly Rollup 4507456 Security Only	Important	Information Disclosure	4503292	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	4507449 Monthly Rollup 4507456 Security Only	Important	Information Disclosure	4503292	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	4507449 Monthly Rollup 4507456	Important	Information Disclosure	4503292	Base: 5.5 Temporal: 5 Vector:	Yes

CVE-2019-1096						
Systems Service Pack 1 (Server Core installation)	Security Only				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	4507449 Monthly Rollup 4507456 Security Only	Important	Information Disclosure	4503292	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	4507449 Monthly Rollup 4507456 Security Only	Important	Information Disclosure	4503292	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	4507452 Monthly	Important	Information Disclosure	4503273	Base: 5.5 Temporal: 5	Yes

CVE-2019-1096						
2008 for 32-bit Systems Service Pack 2 (Server Core installation)	Rollup 4507461 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 2012	4507462 Monthly Rollup 4507464 Security Only	Important	Information Disclosure	4503285	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)	4507462 Monthly Rollup 4507464 Security Only	Important	Information Disclosure	4503285	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	4507448 Monthly Rollup	Important	Information Disclosure	4503276	Base: 5.5 Temporal: 5 Vector:	Yes

CVE-2019-1096						
	4507457 Security Only				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	4507448 Monthly Rollup 4507457 Security Only	Important	Information Disclosure	4503276	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	4507448 Monthly Rollup 4507457 Security Only	Important	Information Disclosure	4503276	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	4507448 Monthly Rollup	Important	Information Disclosure	4503276	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	4507448 Monthly Rollup	Important	Information Disclosure	4503276	Base: 5.5 Temporal: 5 Vector:	Yes

CVE-2019-1096						
(Server Core installation)	4507457 Security Only				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 for 32-bit Systems	4507458 Security Update	Important	Information Disclosure	4503291	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	4507458 Security Update	Important	Information Disclosure	4503291	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	4507460 Security Update	Important	Information Disclosure	4503267	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 32-bit Systems	4507460 Security Update	Important	Information Disclosure	4503267	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-2019-1096						
Windows 10 Version 1607 for x64-based Systems	4507460 Security Update	Important	Information Disclosure	4503267	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)	4507460 Security Update	Important	Information Disclosure	4503267	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	4507450 Security Update	Important	Information Disclosure	4503279	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 x64-based Systems	4507450 Security Update	Important	Information Disclosure	4503279	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	4507455 Security	Important	Information Disclosure	4503284	Base: 5.5 Temporal: 5	Yes

CVE-2019-1096						
1709 for 32-bit 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 x64-based Systems	4507455 Security Update	Important	Information Disclosure	4503284	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	4507435 Security Update	Important	Information Disclosure	4503286	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	4507435 Security Update	Important	Information Disclosure	4503286	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 1803 (Server	4507435 Security Update	Important	Information Disclosure	4503286	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-2019-1096						
Core Installation)						
Windows 10 Version 1803 for ARM64-based Systems	4507435 Security Update	Important	Information Disclosure	4503286	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	4507469 Security Update	Important	Information Disclosure	4503327	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	4507469 Security Update	Important	Information Disclosure	4503327	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-	4507469 Security Update	Important	Information Disclosure	4503327	Base: 5.5 Temporal: 5 Vector:	Yes

CVE-2019-1096						
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 Server 2019	4507469 Security Update	Important	Information Disclosure	4503327	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)	4507469 Security Update	Important	Information Disclosure	4503327	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-based Systems	4507455 Security Update	Important	Information Disclosure	4503284	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	4507453 Security Update	Important	Information Disclosure	4503293	Base: 5.5 Temporal: 5 Vector:	Yes

CVE-2019-1096						
32-bit 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 x64-based Systems	4507453 Security Update	Important	Information Disclosure	4503293	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	4507453 Security Update	Important	Information Disclosure	4503293	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 Core installation)	4507453 Security Update	Important	Information Disclosure	4503293	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	4507452 Monthly Rollup	Important	Information Disclosure	4503273	Base: 5.5 Temporal: 5 Vector:	Yes

CVE-2019-1096						
Itanium-Based Systems Service Pack 2	4507461 Security Only				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 for 32-bit Systems Service Pack 2	4507452 Monthly Rollup 4507461 Security Only	Important	Information Disclosure	4503273	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 Service Pack 2	4507452 Monthly Rollup 4507461 Security Only	Important	Information Disclosure	4503273	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	4507452 Monthly Rollup 4507461	Important	Information Disclosure	4503273	Base: 5.5 Temporal: 5 Vector:	Yes

CVE-2019-1096						
Systems Service Pack 2 (Server Core installation)	Security Only				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	

CVE-2019-1097 - DirectWrite Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1097 MITRE NVD	**CVE Title:** DirectWrite Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when DirectWrite improperly discloses the contents of its memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system. There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document, or by convincing a user to visit an untrusted webpage.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by correcting how DirectWrite 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 memory layout - the vulnerability allows an attacker to collect information that facilitates predicting addressing of the memory. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1097						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4507449 Monthly Rollup 4507456 Security Only	Important	Information Disclosure	4503292	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	4507449 Monthly Rollup 4507456 Security Only	Important	Information Disclosure	4503292	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	4507449 Monthly Rollup 4507456	Important	Information Disclosure	4503292	Base: 5.5 Temporal: 5 Vector:	Yes

CVE-2019-1097						
Systems Service Pack 1 (Server Core installation)	Security Only				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	4507449 Monthly Rollup 4507456 Security Only	Important	Information Disclosure	4503292	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	4507449 Monthly Rollup 4507456 Security Only	Important	Information Disclosure	4503292	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	4507452 Monthly	Important	Information Disclosure	4503273	Base: 5.5 Temporal: 5	Yes

CVE-2019-1097						
2008 for 32-bit Systems Service Pack 2 (Server Core installation)	Rollup 4507461 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 2012	4507462 Monthly Rollup 4507464 Security Only	Important	Information Disclosure	4503285	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)	4507462 Monthly Rollup 4507464 Security Only	Important	Information Disclosure	4503285	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	4507448 Monthly Rollup	Important	Information Disclosure	4503276	Base: 5.5 Temporal: 5 Vector:	Yes

CVE-2019-1097						
	4507457 Security Only				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	4507448 Monthly Rollup 4507457 Security Only	Important	Information Disclosure	4503276	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	4507448 Monthly Rollup 4507457 Security Only	Important	Information Disclosure	4503276	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	4507448 Monthly Rollup	Important	Information Disclosure	4503276	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	4507448 Monthly Rollup	Important	Information Disclosure	4503276	Base: 5.5 Temporal: 5 Vector:	Yes

CVE-2019-1097						
(Server Core installation)	4507457 Security Only				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 for 32-bit Systems	4507458 Security Update	Important	Information Disclosure	4503291	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	4507458 Security Update	Important	Information Disclosure	4503291	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	4507460 Security Update	Important	Information Disclosure	4503267	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 32-bit Systems	4507460 Security Update	Important	Information Disclosure	4503267	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-2019-1097						
Windows 10 Version 1607 for x64-based Systems	4507460 Security Update	Important	Information Disclosure	4503267	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)	4507460 Security Update	Important	Information Disclosure	4503267	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	4507450 Security Update	Important	Information Disclosure	4503279	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 x64-based Systems	4507450 Security Update	Important	Information Disclosure	4503279	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	4507455 Security	Important	Information Disclosure	4503284	Base: 5.5 Temporal: 5	Yes

CVE-2019-1097						
1709 for 32-bit 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 x64-based Systems	4507455 Security Update	Important	Information Disclosure	4503284	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	4507435 Security Update	Important	Information Disclosure	4503286	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	4507435 Security Update	Important	Information Disclosure	4503286	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 1803 (Server	4507435 Security Update	Important	Information Disclosure	4503286	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-2019-1097						
Core Installation)						
Windows 10 Version 1803 for ARM64-based Systems	4507435 Security Update	Important	Information Disclosure	4503286	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	4507469 Security Update	Important	Information Disclosure	4503327	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	4507469 Security Update	Important	Information Disclosure	4503327	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-	4507469 Security Update	Important	Information Disclosure	4503327	Base: 5.5 Temporal: 5 Vector:	Yes

CVE-2019-1097						
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 Server 2019	4507469 Security Update	Important	Information Disclosure	4503327	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)	4507469 Security Update	Important	Information Disclosure	4503327	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-based Systems	4507455 Security Update	Important	Information Disclosure	4503284	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	4507453 Security Update	Important	Information Disclosure	4503293	Base: 5.5 Temporal: 5 Vector:	Yes

CVE-2019-1097						
32-bit 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 x64-based Systems	4507453 Security Update	Important	Information Disclosure	4503293	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	4507453 Security Update	Important	Information Disclosure	4503293	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 Core installation)	4507453 Security Update	Important	Information Disclosure	4503293	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	4507452 Monthly Rollup	Important	Information Disclosure	4503273	Base: 5.5 Temporal: 5 Vector:	Yes

CVE-2019-1097						
Itanium-Based Systems Service Pack 2	4507461 Security Only				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 for 32-bit Systems Service Pack 2	4507452 Monthly Rollup 4507461 Security Only	Important	Information Disclosure	4503273	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 Service Pack 2	4507452 Monthly Rollup 4507461 Security Only	Important	Information Disclosure	4503273	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	4507452 Monthly Rollup 4507461	Important	Information Disclosure	4503273	Base: 5.5 Temporal: 5 Vector:	Yes

CVE-2019-1097						
Systems Service Pack 2 (Server Core installation)	Security Only				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	

CVE-2019-1098 - Windows GDI Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1098 MITRE NVD	**CVE Title:** Windows GDI Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document, or by convincing a user to visit an untrusted webpage. The security update addresses the vulnerability by correcting how the Windows GDI component 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 memory layout - the vulnerability allows an attacker to collect information that facilitates predicting addressing of the memory. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 07/09/2019 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-2019-1098						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4507449 Monthly Rollup 4507456 Security Only	Important	Information Disclosure	4503292	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	4507449 Monthly Rollup 4507456	Important	Information Disclosure	4503292	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-2019-1098						
Service Pack 1	Security Only					
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4507449 Monthly Rollup 4507456 Security Only	Important	Information Disclosure	4503292	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 Itanium-Based Systems Service Pack 1	4507449 Monthly Rollup 4507456 Security Only	Important	Information Disclosure	4503292	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	4507449 Monthly Rollup	Important	Information Disclosure	4503292	Base: 5.5 Temporal: 5	Yes

CVE-2019-1098						
x64-based Systems Service Pack 1	4507456 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 for 32-bit Systems Service Pack 2 (Server Core installation)	4507452 Monthly Rollup 4507461 Security Only	Important	Information Disclosure	4503273	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 Itanium-Based Systems Service Pack 2	4507452 Monthly Rollup 4507461 Security Only	Important	Information Disclosure	4503273	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-2019-1098						
Windows Server 2008 for x64-based Systems Service Pack 2	4507452 Monthly Rollup 4507461 Security Only	Important	Information Disclosure	4503273	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 Service Pack 2 (Server Core installation)	4507452 Monthly Rollup 4507461 Security Only	Important	Information Disclosure	4503273	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-2019-1099 - Windows GDI Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1099 MITRE NVD	**CVE Title:** Windows GDI Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system. There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document, or by convincing a user to visit an untrusted webpage. The security update addresses the vulnerability by correcting how the Windows GDI component 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 memory layout - the vulnerability allows an attacker to collect information that facilitates predicting addressing of the memory. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1099						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4507449 Monthly Rollup 4507456 Security Only	Important	Information Disclosure	4503292	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	4507449 Monthly Rollup 4507456 Security Only	Important	Information Disclosure	4503292	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	4507449 Monthly Rollup 4507456 Security Only	Important	Information Disclosure	4503292	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-2019-1099						
Core installation)						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4507449 Monthly Rollup 4507456 Security Only	Important	Information Disclosure	4503292	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	4507449 Monthly Rollup 4507456 Security Only	Important	Information Disclosure	4503292	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	4507452 Monthly Rollup 4507461 Security Only	Important	Information Disclosure	4503273	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-2019-1099						
Pack 2 (Server Core installation)						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4507452 Monthly Rollup 4507461 Security Only	Important	Information Disclosure	4503273	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	4507452 Monthly Rollup 4507461 Security Only	Important	Information Disclosure	4503273	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	4507452 Monthly Rollup 4507461	Important	Information Disclosure	4503273	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-2019-1099						
Systems Service Pack 2	Security Only					
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4507452 Monthly Rollup 4507461 Security Only	Important	Information Disclosure	4503273	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-2019-1100 - Windows GDI Information Disclosure Vulnerability

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
1100 MITRE NVD	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system. There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document, or by convincing a user to visit an untrusted webpage. The security update addresses the vulnerability by correcting how the Windows GDI component 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 memory layout - the vulnerability allows an attacker to collect information that facilitates predicting addressing of the memory. **Mitigations:** None		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Workarounds: None **Revision:** 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1100						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4507449 Monthly Rollup 4507456 Security Only	Important	Information Disclosure	4503292	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-2019-1100						
Windows 7 for x64-based Systems Service Pack 1	4507449 Monthly Rollup 4507456 Security Only	Important	Information Disclosure	4503292	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 Core installation)	4507449 Monthly Rollup 4507456 Security Only	Important	Information Disclosure	4503292	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 Itanium-Based Systems	4507449 Monthly Rollup 4507456 Security Only	Important	Information Disclosure	4503292	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-2019-1100						
Service Pack 1						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4507449 Monthly Rollup 4507456 Security Only	Important	Information Disclosure	4503292	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 (Server Core installation)	4507452 Monthly Rollup 4507461 Security Only	Important	Information Disclosure	4503273	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 Itanium-	4507452 Monthly Rollup 4507461	Important	Information Disclosure	4503273	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-2019-1100						
Based Systems Service Pack 2	Security Only					
Windows Server 2008 for 32-bit Systems Service Pack 2	4507452 Monthly Rollup 4507461 Security Only	Important	Information Disclosure	4503273	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 Service Pack 2	4507452 Monthly Rollup 4507461 Security Only	Important	Information Disclosure	4503273	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	4507452 Monthly Rollup 4507461 Security	Important	Information Disclosure	4503273	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-2019-1100						
Service Pack 2 (Server Core installation)	Only					

CVE-2019-1101 - Windows GDI Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1101 MITRE NVD	**CVE Title:** Windows GDI Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system. There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document, or by convincing a user to visit an untrusted webpage.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by correcting how the Windows GDI component 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 memory layout - the vulnerability allows an attacker to collect information that facilitates predicting addressing of the memory. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1101						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4507449 Monthly Rollup 4507456 Security Only	Important	Information Disclosure	4503292	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	4507449 Monthly Rollup 4507456 Security Only	Important	Information Disclosure	4503292	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	4507449 Monthly Rollup 4507456	Important	Information Disclosure	4503292	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-2019-1101						
Systems Service Pack 1 (Server Core installation)	Security Only					
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4507449 Monthly Rollup 4507456 Security Only	Important	Information Disclosure	4503292	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	4507449 Monthly Rollup 4507456 Security Only	Important	Information Disclosure	4503292	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	4507452 Monthly	Important	Information Disclosure	4503273	Base: 5.5 Temporal: 5	Yes

CVE-2019-1101						
2008 for 32-bit Systems Service Pack 2 (Server Core installation)	Rollup 4507461 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 for Itanium-Based Systems Service Pack 2	4507452 Monthly Rollup 4507461 Security Only	Important	Information Disclosure	4503273	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	4507452 Monthly Rollup 4507461 Security Only	Important	Information Disclosure	4503273	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-2019-1101						
Windows Server 2008 for x64-based Systems Service Pack 2	4507452 Monthly Rollup 4507461 Security Only	Important	Information Disclosure	4503273	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 Service Pack 2 (Server Core installation)	4507452 Monthly Rollup 4507461 Security Only	Important	Information Disclosure	4503273	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-2019-1102 - GDI+ Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1102 MITRE NVD	**CVE Title:** GDI+ Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory. An attacker who successfully exploited this vulnerability 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. There are multiple ways an attacker could exploit the vulnerability: • In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability and then convince users to view the website. An attacker would have no way to force users to view the attacker-controlled content. Instead, an attacker would have to convince users to take action, typically by getting them to open an email attachment or click a link in an email or instant message.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	• In a file-sharing attack scenario, an attacker could provide a specially crafted document file that is designed to exploit the vulnerability, and then convince users to open the document file. The security update addresses the vulnerability by correcting the way that the Windows GDI handles objects in the memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1102						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4507449 Monthly Rollup 4507456 Security Only	Critical	Remote Code Execution	4503292	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/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	4507449 Monthly Rollup 4507456 Security Only	Critical	Remote Code Execution	4503292	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based	4507449 Monthly Rollup 4507456	Critical	Remote Code Execution	4503292	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1102						
Systems Service Pack 1 (Server Core installation)	Security Only					
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4507449 Monthly Rollup 4507456 Security Only	Critical	Remote Code Execution	4503292	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/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	4507449 Monthly Rollup 4507456 Security Only	Critical	Remote Code Execution	4503292	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit	4507452 Monthly Rollup	Critical	Remote Code Execution	4503273	Base: 8.4 Temporal: 7.6	Yes

CVE-2019-1102						
Systems Service Pack 2 (Server Core installation)	4507461 Security Only				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2012	4507462 Monthly Rollup 4507464 Security Only	Critical	Remote Code Execution	4503285	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4507462 Monthly Rollup 4507464 Security Only	Critical	Remote Code Execution	4503285	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4507448 Monthly Rollup 4507457 Security Only	Critical	Remote Code Execution	4503276	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1102						
Windows 8.1 for x64-based systems	4507448 Monthly Rollup 4507457 Security Only	Critical	Remote Code Execution	4503276	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4507448 Monthly Rollup 4507457 Security Only	Critical	Remote Code Execution	4503276	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4507448 Monthly Rollup 4507457 Security Only	Critical	Remote Code Execution	4503276	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4507458 Security Update	Critical	Remote Code Execution	4503291	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1102						
Windows 10 for x64-based Systems	4507458 Security Update	Critical	Remote Code Execution	4503291	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4507460 Security Update	Critical	Remote Code Execution	4503267	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/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	4507460 Security Update	Critical	Remote Code Execution	4503267	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/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	4507460 Security Update	Critical	Remote Code Execution	4503267	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4507460 Security Update	Critical	Remote Code Execution	4503267	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1102						
Windows 10 Version 1703 for 32-bit Systems	4507450 Security Update	Critical	Remote Code Execution	4503279	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/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	4507450 Security Update	Critical	Remote Code Execution	4503279	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/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	4507455 Security Update	Critical	Remote Code Execution	4503284	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/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	4507455 Security Update	Critical	Remote Code Execution	4503284	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/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	4507435 Security Update	Critical	Remote Code Execution	4503286	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1102						
Windows 10 Version 1803 for x64-based Systems	4507435 Security Update	Critical	Remote Code Execution	4503286	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4507435 Security Update	Critical	Remote Code Execution	4503286	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/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	4507435 Security Update	Critical	Remote Code Execution	4503286	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/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	4507469 Security Update	Critical	Remote Code Execution	4503327	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for	4507469 Security Update	Critical	Remote Code Execution	4503327	Base: 8.4 Temporal: 7.6	Yes

CVE-2019-1102						
x64-based Systems					Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1809 for ARM64-based Systems	4507469 Security Update	Critical	Remote Code Execution	4503327	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4507469 Security Update	Critical	Remote Code Execution	4503327	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4507469 Security Update	Critical	Remote Code Execution	4503327	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/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	4507455 Security Update	Critical	Remote Code Execution	4503284	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1102						
Windows 10 Version 1903 for 32-bit Systems	4507453 Security Update	Critical	Remote Code Execution	4503293	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/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	4507453 Security Update	Critical	Remote Code Execution	4503293	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/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	4507453 Security Update	Critical	Remote Code Execution	4503293	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4507453 Security Update	Critical	Remote Code Execution	4503293	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-	4507452 Monthly Rollup	Critical	Remote Code Execution	4503273	Base: 8.4 Temporal: 7.6	Yes

CVE-2019-1102						
Based Systems Service Pack 2	4507461 Security Only				Vector: CVSS:3.0/AV:L/AC:L/PR:N/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	4507452 Monthly Rollup 4507461 Security Only	Critical	Remote Code Execution	4503273	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/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	4507452 Monthly Rollup 4507461 Security Only	Critical	Remote Code Execution	4503273	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/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	4507452 Monthly Rollup 4507461 Security Only	Critical	Remote Code Execution	4503273	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1102						
2 (Server Core installation)						

CVE-2019-1103 - Chakra Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1103 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.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 **Workarounds:** None **Revision:** 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1103						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4507458 Security Update	Critical	Remote Code Execution	4503291	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 on Windows 10 for x64-based Systems	4507458 Security Update	Critical	Remote Code Execution	4503291	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 on Windows Server 2016	4507460 Security Update	Moderate	Remote Code Execution	4503267	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-2019-1103						
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4507460 Security Update	Critical	Remote Code Execution	4503267	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 on Windows 10 Version 1607 for x64-based Systems	4507460 Security Update	Critical	Remote Code Execution	4503267	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 on Windows 10 Version 1703 for 32-bit Systems	4507450 Security Update	Critical	Remote Code Execution	4503279	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-2019-1103						
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4507450 Security Update	Critical	Remote Code Execution	4503279	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 on Windows 10 Version 1709 for 32-bit Systems	4507455 Security Update	Critical	Remote Code Execution	4503284	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 on Windows 10 Version 1709 for x64-based Systems	4507455 Security Update	Critical	Remote Code Execution	4503284	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-2019-1103						
Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems	4507435 Security Update	Critical	Remote Code Execution	4503286	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 on Windows 10 Version 1803 for x64-based Systems	4507435 Security Update	Critical	Remote Code Execution	4503286	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 on Windows 10 Version 1803 for ARM64-based Systems	4507435 Security Update	Critical	Remote Code Execution	4503286	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-2019-1103						
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems	4507469 Security Update	Critical	Remote Code Execution	4503327	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 on Windows 10 Version 1809 for x64-based Systems	4507469 Security Update	Critical	Remote Code Execution	4503327	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 on Windows 10 Version 1809 for ARM64-based Systems	4507469 Security Update	Critical	Remote Code Execution	4503327	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-2019-1103						
Microsoft Edge on Windows Server 2019	4507469 Security Update	Moderate	Remote Code Execution	4503327	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 on Windows 10 Version 1709 for ARM64-based Systems	4507455 Security Update	Critical	Remote Code Execution	4503284	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 on Windows 10 Version 1903 for 32-bit Systems	4507453 Security Update	Critical	Remote Code Execution	4503293	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 on Windows 10 Version	4507453 Security Update	Critical	Remote Code Execution	4503293	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-2019-1103						
1903 for x64-based Systems						
Microsoft Edge on Windows 10 Version 1903 for ARM64-based Systems	4507453 Security Update	Critical	Remote Code Execution	4503293	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	4503293	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1104 - Microsoft Browser Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1104 MITRE NVD	**CVE Title:** Microsoft Browser Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that Microsoft browsers access objects in memory. The vulnerability could corrupt memory in a way that could allow an attacker to 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. An attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft browsers, 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. In all cases, however, an attacker would have no way to force users to view the attacker-controlled content. Instead, an attacker would have to convince users to take action, typically via an enticement in email or instant message, or by getting them to open an email attachment.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by modifying how Microsoft browsers handle objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1104						
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	4507434 IE Cumulative 4507452 Monthly Rollup	Moderate	Remote Code Execution	4503273	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 9 on Windows Server 2008 for x64-based Systems Service Pack 2	4507434 IE Cumulative 4507452 Monthly Rollup	Moderate	Remote Code Execution	4503273	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-2019-1104						
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1	4507434 IE Cumulative 4507449 Monthly Rollup	Critical	Remote Code Execution	4503292	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 7 for x64-based Systems Service Pack 1	4507434 IE Cumulative 4507449 Monthly Rollup	Critical	Remote Code Execution	4503292	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	4507434 IE Cumulative 4507449 Monthly	Moderate	Remote Code Execution	4503292	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-2019-1104						
Server 2008 R2 for x64-based Systems Service Pack 1	Rollup					
Internet Explorer 11 on Windows Server 2012	4507434 IE Cumulative	Moderate	Remote Code Execution	4503259	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	4507448 Monthly Rollup 4507434 IE Cumulative	Critical	Remote Code Execution	4503259	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	4507448 Monthly Rollup	Critical	Remote Code Execution	4503259	Base: 7.5 Temporal: 6.7	Yes

CVE-2019-1104						
Windows 8.1 for x64-based systems	4507434 IE Cumulative				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 2012 R2	4507448 Monthly Rollup 4507434 IE Cumulative	Moderate	Remote Code Execution	4503259	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	4507448 Monthly Rollup	Critical	Remote Code Execution	4503276	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	4507458 Security Update	Critical	Remote Code Execution	4503291	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-2019-1104						
Internet Explorer 11 on Windows 10 for x64-based Systems	4507458 Security Update	Critical	Remote Code Execution	4503291	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 2016	4507460 Security Update	Moderate	Remote Code Execution	4503267	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	4507460 Security Update	Critical	Remote Code Execution	4503267	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-2019-1104						
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4507460 Security Update	Critical	Remote Code Execution	4503267	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 32-bit Systems	4507450 Security Update	Critical	Remote Code Execution	4503279	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	4507450 Security Update	Critical	Remote Code Execution	4503279	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-2019-1104						
10 Version 1703 for x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems	4507455 Security Update	Critical	Remote Code Execution	4503284	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-	4507455 Security Update	Critical	Remote Code Execution	4503284	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-2019-1104						
based Systems						
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems	4507435 Security Update	Critical	Remote Code Execution	4503286	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	4507435 Security Update	Critical	Remote Code Execution	4503286	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-2019-1104						
Internet Explorer 11 on Windows 10 Version 1803 for ARM64-based Systems	4507435 Security Update	Critical	Remote Code Execution	4503286	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 32-bit Systems	4507469 Security Update	Critical	Remote Code Execution	4503327	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	4507469 Security Update	Critical	Remote Code Execution	4503327	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-2019-1104						
10 Version 1809 for x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems	4507469 Security Update	Critical	Remote Code Execution	4503327	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	4507469 Security Update	Moderate	Remote Code Execution	4503327	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-2019-1104						
Internet Explorer 11 on Windows 10 Version 1709 for ARM64-based Systems	4507455 Security Update	Critical	Remote Code Execution	4503284	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 32-bit Systems	4507453 Security Update	Critical	Remote Code Execution	4503293	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	4507453 Security Update	Critical	Remote Code Execution	4503293	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-2019-1104						
10 Version 1903 for x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1903 for ARM64-based Systems	4507453 Security Update	Critical	Remote Code Execution	4503293	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	4507462 Monthly Rollup 4507434 IE Cumulative	Moderate	Remote Code Execution	4503259	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-2019-1104						
Microsoft Edge on Windows 10 for 32-bit Systems	4507458 Security Update	Critical	Remote Code Execution	4503291	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 on Windows 10 for x64-based Systems	4507458 Security Update	Critical	Remote Code Execution	4503291	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 on Windows Server 2016	4507460 Security Update	Moderate	Remote Code Execution	4503267	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 on Windows 10 Version	4507460 Security Update	Critical	Remote Code Execution	4503267	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-2019-1104						
1607 for 32-bit Systems						
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4507460 Security Update	Critical	Remote Code Execution	4503267	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 on Windows 10 Version 1703 for 32-bit Systems	4507450 Security Update	Critical	Remote Code Execution	4503279	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 on Windows	4507450 Security Update	Critical	Remote Code Execution	4503279	Base: 4.2 Temporal: 3.8	Yes

CVE-2019-1104						
10 Version 1703 for x64-based Systems					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 on Windows 10 Version 1709 for 32-bit Systems	4507455 Security Update	Critical	Remote Code Execution	4503284	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 on Windows 10 Version 1709 for x64-based Systems	4507455 Security Update	Critical	Remote Code Execution	4503284	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-2019-1104						
Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems	4507435 Security Update	Critical	Remote Code Execution	4503286	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 on Windows 10 Version 1803 for x64-based Systems	4507435 Security Update	Critical	Remote Code Execution	4503286	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 on Windows 10 Version 1803 for	4507435 Security Update	Critical	Remote Code Execution	4503286	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-2019-1104						
ARM64-based Systems						
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems	4507469 Security Update	Critical	Remote Code Execution	4503327	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 on Windows 10 Version 1809 for x64-based Systems	4507469 Security Update	Critical	Remote Code Execution	4503327	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 on Windows	4507469 Security Update	Critical	Remote Code Execution	4503327	Base: 4.2 Temporal: 3.8	Yes

CVE-2019-1104						
10 Version 1809 for ARM64-based Systems					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 on Windows Server 2019	4507469 Security Update	Moderate	Remote Code Execution	4503327	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 on Windows 10 Version 1709 for ARM64-based Systems	4507455 Security Update	Critical	Remote Code Execution	4503284	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 on Windows	4507453 Security Update	Critical	Remote Code Execution	4503293	Base: 4.2 Temporal: 3.8	Yes

CVE-2019-1104						
10 Version 1903 for 32-bit Systems					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 on Windows 10 Version 1903 for x64-based Systems	4507453 Security Update	Critical	Remote Code Execution	4503293	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 on Windows 10 Version 1903 for ARM64-based Systems	4507453 Security Update	Critical	Remote Code Execution	4503293	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-2019-1106 - Chakra Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1106 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 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1106						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows Server 2016	4507460 Security Update	Moderate	Remote Code Execution	4503267	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 on Windows 10 Version 1607 for 32-bit Systems	4507460 Security Update	Critical	Remote Code Execution	4503267	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 on Windows 10 Version 1607 for x64-based Systems	4507460 Security Update	Critical	Remote Code Execution	4503267	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 on Windows	4507450 Security Update	Critical	Remote Code Execution	4503279	Base: 4.2 Temporal: 3.8	Yes

CVE-2019-1106						
10 Version 1703 for 32-bit Systems					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 on Windows 10 Version 1703 for x64-based Systems	4507450 Security Update	Critical	Remote Code Execution	4503279	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 on Windows 10 Version 1709 for 32-bit Systems	4507455 Security Update	Critical	Remote Code Execution	4503284	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 on Windows 10 Version 1709 for	4507455 Security Update	Critical	Remote Code Execution	4503284	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-2019-1106						
x64-based Systems						
Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems	4507435 Security Update	Critical	Remote Code Execution	4503286	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 on Windows 10 Version 1803 for x64-based Systems	4507435 Security Update	Critical	Remote Code Execution	4503286	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 on Windows 10 Version 1803 for ARM64-	4507435 Security Update	Critical	Remote Code Execution	4503286	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-2019-1106						
based Systems						
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems	4507469 Security Update	Critical	Remote Code Execution	4503327	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 on Windows 10 Version 1809 for x64-based Systems	4507469 Security Update	Critical	Remote Code Execution	4503327	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 on Windows 10 Version 1809 for ARM64-	4507469 Security Update	Critical	Remote Code Execution	4503327	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-2019-1106						
based Systems						
Microsoft Edge on Windows Server 2019	4507469 Security Update	Moderate	Remote Code Execution	4503327	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 on Windows 10 Version 1709 for ARM64-based Systems	4507455 Security Update	Critical	Remote Code Execution	4503284	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 on Windows 10 Version 1903 for 32-bit Systems	4507453 Security Update	Critical	Remote Code Execution	4503293	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-2019-1106						
Microsoft Edge on Windows 10 Version 1903 for x64-based Systems	4507453 Security Update	Critical	Remote Code Execution	4503293	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 on Windows 10 Version 1903 for ARM64-based Systems	4507453 Security Update	Critical	Remote Code Execution	4503293	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	4503293	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1107 - Chakra Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1107 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 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1107						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4507458 Security Update	Critical	Remote Code Execution	4503291	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 on Windows 10 for x64-based Systems	4507458 Security Update	Critical	Remote Code Execution	4503291	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 on Windows Server 2016	4507460 Security Update	Moderate	Remote Code Execution	4503267	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 on Windows 10 Version 1607 for	4507460 Security Update	Critical	Remote Code Execution	4503267	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-2019-1107						
32-bit Systems						
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4507460 Security Update	Critical	Remote Code Execution	4503267	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 on Windows 10 Version 1703 for 32-bit Systems	4507450 Security Update	Critical	Remote Code Execution	4503279	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 on Windows 10 Version 1703 for x64-based Systems	4507450 Security Update	Critical	Remote Code Execution	4503279	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-2019-1107						
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4507455 Security Update	Critical	Remote Code Execution	4503284	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 on Windows 10 Version 1709 for x64-based Systems	4507455 Security Update	Critical	Remote Code Execution	4503284	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 on Windows 10 Version 1803 for 32-bit Systems	4507435 Security Update	Critical	Remote Code Execution	4503286	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-2019-1107						
Microsoft Edge on Windows 10 Version 1803 for x64-based Systems	4507435 Security Update	Critical	Remote Code Execution	4503286	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 on Windows 10 Version 1803 for ARM64-based Systems	4507435 Security Update	Critical	Remote Code Execution	4503286	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 on Windows 10 Version 1809 for 32-bit Systems	4507469 Security Update	Critical	Remote Code Execution	4503327	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-2019-1107						
Microsoft Edge on Windows 10 Version 1809 for x64-based Systems	4507469 Security Update	Critical	Remote Code Execution	4503327	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 on Windows 10 Version 1809 for ARM64-based Systems	4507469 Security Update	Critical	Remote Code Execution	4503327	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 on Windows Server 2019	4507469 Security Update	Moderate	Remote Code Execution	4503327	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 on Windows 10 Version	4507455 Security Update	Critical	Remote Code Execution	4503284	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-2019-1107						
1709 for ARM64-based Systems						
Microsoft Edge on Windows 10 Version 1903 for 32-bit Systems	4507453 Security Update	Critical	Remote Code Execution	4503293	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 on Windows 10 Version 1903 for x64-based Systems	4507453 Security Update	Critical	Remote Code Execution	4503293	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 on Windows 10 Version 1903 for	4507453 Security Update	Critical	Remote Code Execution	4503293	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-2019-1107						
ARM64-based Systems						
ChakraCore	Release Notes Security Update	Critical	Remote Code Execution	4503293	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1108 - Remote Desktop Protocol Client Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1108 MITRE NVD	**CVE Title:** Remote Desktop Protocol Client Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the Windows RDP client improperly discloses the contents of its memory. An attacker who successfully	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	exploited this vulnerability could obtain information to further compromise the userâ€™s system. To exploit this vulnerability, an attacker would have to connect remotely to an affected system and run a specially crafted application. The security update addresses the vulnerability by correcting how the Windows RDP client initializes 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. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 07/09/2019 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-2019-1108						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4507449 Monthly Rollup 4507456 Security Only	Important	Information Disclosure	4503292	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1108						
Windows 7 for x64-based Systems Service Pack 1	4507449 Monthly Rollup 4507456 Security Only	Important	Information Disclosure	4503292	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/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 Core installation)	4507449 Monthly Rollup 4507456 Security Only	Important	Information Disclosure	4503292	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/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 Itanium-Based	4507449 Monthly Rollup 450745	Important	Information Disclosure	4503292	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1108						
Systems Service Pack 1	6 Security Only					
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4507449 Monthly Rollup 4507456 Security Only	Important	Information Disclosure	4503292	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/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 (Server Core installation)	4507452 Monthly Rollup 4507461 Security Only	Important	Information Disclosure	4503273	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1108						
Windows Server 2012	4507462 Monthly Rollup 4507464 Security Only	Important	Information Disclosure	4503285	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/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)	4507462 Monthly Rollup 4507464 Security Only	Important	Information Disclosure	4503285	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/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	4507448 Monthly Rollup 4507457 Security	Important	Information Disclosure	4503276	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1108						
	Only					
Windows 8.1 for x64-based systems	4507448 Monthly Rollup 4507457 Security Only	Important	Information Disclosure	4503276	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/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	4507448 Monthly Rollup 4507457 Security Only	Important	Information Disclosure	4503276	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/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	4507448 Monthly Rollup	Important	Information Disclosure	4503276	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1108						
Windows Server 2012 R2 (Server Core installation)	4507448 Monthly Rollup 4507457 Security Only	Important	Information Disclosure	4503276	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/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	4507458 Security Update	Important	Information Disclosure	4503291	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/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	4507458 Security Update	Important	Information Disclosure	4503291	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4507460 Security Update	Important	Information Disclosure	4503267	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1108						
Windows 10 Version 1607 for 32-bit Systems	4507460 Security Update	Important	Information Disclosure	4503267	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/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	4507460 Security Update	Important	Information Disclosure	4503267	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/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)	4507460 Security Update	Important	Information Disclosure	4503267	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/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	4507450 Security Update	Important	Information Disclosure	4503279	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1108						
Windows 10 Version 1703 for x64-based Systems	4507450 Security Update	Important	Information Disclosure	4503279	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/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 32-bit Systems	4507455 Security Update	Important	Information Disclosure	4503284	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/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	4507455 Security Update	Important	Information Disclosure	4503284	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/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	4507435 Security Update	Important	Information Disclosure	4503286	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/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	4507435 Security	Important	Information Disclosure	4503286	Base: 6.5 Temporal: 5.9 Vector:	Yes

CVE-2019-1108						
x64-based Systems	Update				CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server, version 1803 (Server Core Installation)	4507435 Security Update	Important	Information Disclosure	4503286	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/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	4507435 Security Update	Important	Information Disclosure	4503286	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/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	4507469 Security Update	Important	Information Disclosure	4503327	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1108						
Windows 10 Version 1809 for x64-based Systems	4507469 Security Update	Important	Information Disclosure	4503327	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/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	4507469 Security Update	Important	Information Disclosure	4503327	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2019	4507469 Security Update	Important	Information Disclosure	4503327	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/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)	4507469 Security Update	Important	Information Disclosure	4503327	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1108						
Windows 10 Version 1709 for ARM64-based Systems	4507455 Security Update	Important	Information Disclosure	4503284	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/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	4507453 Security Update	Important	Information Disclosure	4503293	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/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	4507453 Security Update	Important	Information Disclosure	4503293	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/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	4507453 Security Update	Important	Information Disclosure	4503293	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1108						
Windows Server, version 1903 (Server Core installation)	4507453 Security Update	Important	Information Disclosure	4503293	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/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 Itanium-Based Systems Service Pack 2	4507452 Monthly Rollup 4507461 Security Only	Important	Information Disclosure	4503273	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/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	4507452 Monthly Rollup 4507461 Security Only	Important	Information Disclosure	4503273	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1108						
Windows Server 2008 for x64-based Systems Service Pack 2	4507452 Monthly Rollup 4507461 Security Only	Important	Information Disclosure	4503273	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/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 Service Pack 2 (Server Core installation)	4507452 Monthly Rollup 4507461 Security Only	Important	Information Disclosure	4503273	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1109 - Microsoft Office Spoofing Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1109 MITRE NVD	**CVE Title:** Microsoft Office Spoofing Vulnerability **Description:** A spoofing vulnerability exists when Microsoft Office Javascript does not check the validity of the web page making a request to Office documents. An attacker who successfully exploited this vulnerability could read or write information in Office documents. The security update addresses the vulnerability by correcting the way that Microsoft Office Javascript verifies trusted web pages. **FAQ:** **Is the Preview Pane an attack vector for this vulnerability?** Maybe. If a user has installed an Office Add-in, and then opens an email that uses the add-in in the Preview Pane, ads embedded in the add-in can cause the Preview Pane to become an attack vector. **Mitigations:**	Important	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Workarounds:** None **Revision:** 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1109						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Office 2013 Service Pack 1 (32-bit editions)	4018375 Security Update	Important	Spoofing	3039782	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2013 Service Pack 1 (64-bit editions)	4018375 Security Update	Important	Spoofing	3039782	Base: N/A Temporal:	Maybe

CVE-2019-1109						
					N/A Vector: N/A	
Microsoft Office 2013 RT Service Pack 1	4018375 Security Update	Important	Spoofing	3039782	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 (32-bit edition)	4464534 Security Update	Important	Spoofing	3039782	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 (64-bit edition)	4464534 Security Update	Important	Spoofing	3039782	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2019 for 32-bit editions	Click to Run Security Update	Important	Spoofing	3039782	Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Office 2019 for 64-bit editions	Click to Run Security Update	Important	Spoofing	3039782	Base: N/A Temporal: N/A Vector: N/A	No

CVE-2019-1109						
Office 365 ProPlus for 32-bit Systems	Click to Run Security Update	Important	Spoofing	3039782	Base: N/A Temporal: N/A Vector: N/A	No
Office 365 ProPlus for 64-bit Systems	Click to Run Security Update	Important	Spoofing	3039782	Base: N/A Temporal: N/A Vector: N/A	No

CVE-2019-1110 - Microsoft Excel Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1110 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	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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. **FAQ:** **Is the Preview Pane an attack vector for this vulnerability?** No, the Preview Pane is not an attack vector.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Are the updates for the Microsoft Office for Mac currently available? The security update for Microsoft Office 2016 for Mac and Microsoft Office 2019 for Mac are not immediately available. The updates will be released as soon as possible, and when they are available, customers will be notified via a revision to this CVE information. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1110						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Excel 2010 Service Pack 2 (32-bit editions)	4464572 Security Update	Important	Remote Code Execution	4462230	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2010 Service Pack 2 (64-bit editions)	4464572 Security Update	Important	Remote Code Execution	4462230	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2013 Service Pack 1 (32-bit editions)	4464565 Security Update	Important	Remote Code Execution	4462209	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2013 Service Pack 1 (64-bit editions)	4464565 Security Update	Important	Remote Code Execution	4462209	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2013 RT Service Pack 1	4464565 Security Update	Important	Remote Code Execution	4462209	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1110						
Microsoft Office 2016 for Mac		Important	Remote Code Execution	4462209	Base: N/A Temporal: N/A Vector: N/A	
Microsoft Excel 2016 (32-bit edition)	4475513 Security Update	Important	Remote Code Execution	4462236	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2016 (64-bit edition)	4475513 Security Update	Important	Remote Code Execution	4462236	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	4462236	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	4462236	Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Office 2019 for Mac		Important	Remote Code Execution	4462236	Base: N/A Temporal:	

CVE-2019-1110						
					N/A Vector: N/A	
Office 365 ProPlus for 32-bit Systems	Click to Run Security Update	Important	Remote Code Execution	4462236	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	4462236	Base: N/A Temporal: N/A Vector: N/A	No

CVE-2019-1111 - Microsoft Excel Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1111 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	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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. **FAQ:** **Is the Preview Pane an attack vector for this vulnerability?**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	No, the Preview Pane is not an attack vector. **Are the updates for the Microsoft Office for Mac currently available?** The security update for Microsoft Office 2016 for Mac and Microsoft Office 2019 for Mac are not immediately available. The updates will be released as soon as possible, and when they are available, customers will be notified via a revision to this CVE information. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1111						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Excel 2010 Service Pack 2 (32-bit editions)	4464572 Security Update	Important	Remote Code Execution	4462230	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2010 Service Pack 2 (64-bit editions)	4464572 Security Update	Important	Remote Code Execution	4462230	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (32-bit editions)	4462224 Security Update	Important	Remote Code Execution	4462177	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (64-bit editions)	4462224 Security Update	Important	Remote Code Execution	4462177	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1111						
Microsoft Office 2013 Service Pack 1 (32-bit editions)	4464543 Security Update	Important	Remote Code Execution	4022237	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2013 Service Pack 1 (64-bit editions)	4464543 Security Update	Important	Remote Code Execution	4022237	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2013 RT Service Pack 1	4464543 Security Update	Important	Remote Code Execution	4022237	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2013 Service Pack 1 (32-bit editions)	4464565 Security Update	Important	Remote Code Execution	4462209	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2013 Service Pack 1 (64-bit editions)	4464565 Security Update	Important	Remote Code Execution	4462209	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2013 RT Service Pack 1	4464565 Security Update	Important	Remote Code Execution	4462209	Base: N/A Temporal:	Maybe

CVE-2019-1111						
					N/A Vector: N/A	
Microsoft Office 2016 for Mac		Important	Remote Code Execution	4462209	Base: N/A Temporal: N/A Vector: N/A	
Microsoft Excel 2016 (32-bit edition)	4475513 Security Update	Important	Remote Code Execution	4462236	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2016 (64-bit edition)	4475513 Security Update	Important	Remote Code Execution	4462236	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 (32-bit edition)	4461539 Security Update	Important	Remote Code Execution	4022232	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 (64-bit edition)	4461539 Security Update	Important	Remote Code Execution	4022232	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1111						
Microsoft Office 2019 for 32-bit editions	Click to Run Security Update	Important	Remote Code Execution	4022232	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	4022232	Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Office 2019 for Mac		Important	Remote Code Execution	4022232	Base: N/A Temporal: N/A Vector: N/A	
Office 365 ProPlus for 32-bit Systems	Click to Run Security Update	Important	Remote Code Execution	4022232	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	4022232	Base: N/A Temporal: N/A Vector: N/A	No

CVE-2019-1112 - Microsoft Excel Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1112 MITRE NVD	**CVE Title:** Microsoft Excel Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when Microsoft Excel improperly discloses the contents of its memory. An attacker who exploited the vulnerability could use the information to compromise the userâ€™s computer or data. To exploit the vulnerability, an attacker could craft a special document file and then convince the user to open it. An attacker must know the memory address location where the object was created. The update addresses the vulnerability by changing the way certain Excel functions 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 unauthorized file system access - reading from the file system.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1112						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2019-1112						
Microsoft Office 2019 for 32-bit editions	Click to Run Security Update	Important	Information Disclosure		Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Office 2019 for 64-bit editions	Click to Run Security Update	Important	Information Disclosure		Base: N/A Temporal: N/A Vector: N/A	No
Office 365 ProPlus for 32-bit Systems	Click to Run Security Update	Important	Information Disclosure		Base: N/A Temporal: N/A Vector: N/A	No
Office 365 ProPlus for 64-bit Systems	Click to Run Security Update	Important	Information Disclosure		Base: N/A Temporal: N/A Vector: N/A	No

CVE-2019-1113 - .NET Framework Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1113 MITRE NVD	**CVE Title:** .NET Framework Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in .NET software when the software fails to check the source markup of a file. 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 .NET Framework. 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. The security update addresses the vulnerability by correcting how .NET Framework checks the source markup of a file.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: **There are two updates for .NET Framework 3.5 installed on Windows 10 version 1809 and Windows Server 2019. How do I know which update I need to install?** The security updates for Windows 10 version 1809 and Windows Server 2019 include both .NET Framework 3.5 and 4.7.2 or 4.8. Customers running these versions of Windows 10 need to determine if they are also running .NET Framework 4.7.2 or .NET Framework 4.8. Install the security update that includes that second version of .NET Framework. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1113						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft .NET Framework 4.5.2 on Windows 7 for 32-bit Systems Service Pack 1	4507420 Monthly Rollup 4507411 Security Only	Critical	Remote Code Execution	4503865	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows 7 for x64-based Systems Service Pack 1	4507420 Monthly Rollup 4507411 Security Only	Critical	Remote Code Execution	4503865	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4507420 Monthly Rollup 4507411	Critical	Remote Code Execution	4503865	Base: N/A Temporal: N/A	Maybe

CVE-2019-1113						
	Security Only				Vector: N/A	
Microsoft .NET Framework 4.5.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4507420 Monthly Rollup 4507411 Security Only	Critical	Remote Code Execution	4503865	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2012	4507412 Security Only 4507421 Monthly Rollup	Critical	Remote Code Execution	4499407; 4503866	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2012 (Server Core installation)	4507412 Security Only 4507421 Monthly Rollup	Critical	Remote Code Execution	4499407; 4503866	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows 8.1 for 32-bit systems	4507413 Security Only	Critical	Remote Code Execution	4499408; 4503867	Base: N/A Temporal: N/A	Maybe

CVE-2019-1113						
	4507422 Monthly Rollup				Vector: N/A	
Microsoft .NET Framework 4.5.2 on Windows 8.1 for x64-based systems	4507413 Security Only 4507422 Monthly Rollup	Critical	Remote Code Execution	4499408; 4503867	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2012 R2	4507413 Security Only 4507422 Monthly Rollup	Critical	Remote Code Execution	4499408; 4503867	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows RT 8.1	4507422 Monthly Rollup	Critical	Remote Code Execution	4499408; 4503867	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2012 R2 (Server Core installation)	4507413 Security Only	Critical	Remote Code Execution	4499408; 4503867	Base: N/A Temporal: N/A	Maybe

CVE-2019-1113						
	4507422 Monthly Rollup				Vector: N/A	
Microsoft .NET Framework 4.5.2 on Windows Server 2008 for 32-bit Systems Service Pack 2	4507423 Monthly Rollup 4507414 Security Only	Critical	Remote Code Execution	4489489; 4499409	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2008 for x64-based Systems Service Pack 2	4507423 Monthly Rollup 4507414 Security Only	Critical	Remote Code Execution	4489489; 4499409	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6 on Windows Server 2008 for 32-bit Systems Service Pack 2	4507423 Monthly Rollup 4507414 Security Only	Critical	Remote Code Execution	4489489; 4499409	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1113						
Microsoft .NET Framework 4.6 on Windows Server 2008 for x64-based Systems Service Pack 2	4507423 Monthly Rollup 4507414 Security Only	Critical	Remote Code Execution	4489489; 4499409	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Visual Studio 2017	Release Notes Security Update	Critical	Remote Code Execution	4489489; 4499409	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2 on Windows 10 for 32-bit Systems	4507458 Security Update	Critical	Remote Code Execution	4503291	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.6/4.6.1/4.6.2 on Windows 10 for x64-based Systems	4507458 Security Update	Critical	Remote Code Execution	4503291	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-1113						
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 7 for 32-bit Systems Service Pack 1	4507420 Monthly Rollup 4507411 Security Only	Critical	Remote Code Execution	4503291	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 7 for x64-based Systems Service Pack 1	4507420 Monthly Rollup 4507411 Security Only	Critical	Remote Code Execution	4503291	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4507420 Monthly Rollup 4507411 Security Only	Critical	Remote Code Execution	4503291	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4507420 Monthly Rollup 4507411 Security	Critical	Remote Code Execution	4503291	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1113						
	Only					
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012	4507421 Monthly Rollup 4507412 Security Only	Critical	Remote Code Execution	4499407; 4503866	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012 (Server Core installation)	4507421 Monthly Rollup 4507412 Security Only	Critical	Remote Code Execution	4499407; 4503866	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 8.1 for 32-bit systems	4507413 Security Only 4507422 Monthly Rollup	Critical	Remote Code Execution	4499408; 4503867	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 8.1 for x64-based systems	4507422 Monthly Rollup 4507413	Critical	Remote Code Execution	4499408; 4503867	Base: N/A Temporal: N/A	Maybe

CVE-2019-1113						
	Security Only				Vector: N/A	
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012 R2	4507422 Monthly Rollup 4507413 Security Only	Critical	Remote Code Execution	4499408; 4503867	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows RT 8.1	4507422 Monthly Rollup	Critical	Remote Code Execution	4499408; 4503867	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012 R2 (Server Core installation)	4507422 Monthly Rollup 4507413 Security Only	Critical	Remote Code Execution	4499408; 4503867	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Visual Studio 2017 version 15.9	Release Notes Security Update	Critical	Remote Code Execution	4499408; 4503867	Base: N/A Temporal: N/A	Maybe

CVE-2019-1113						
					Vector: N/A	
Microsoft .NET Framework 4.8 on Windows 7 for 32-bit Systems Service Pack 1	4507420 Monthly Rollup 4507411 Security Only	Critical	Remote Code Execution	4499406; 4503865	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 7 for x64-based Systems Service Pack 1	4507420 Monthly Rollup 4507411 Security Only	Critical	Remote Code Execution	4499406; 4503865	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4507420 Monthly Rollup 4507411 Security Only	Critical	Remote Code Execution	4499406; 4503865	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4507420 Monthly Rollup	Critical	Remote Code Execution	4499406; 4503865	Base: N/A Temporal: N/A	Maybe

CVE-2019-1113						
	4507411 Security Only				Vector: N/A	
Microsoft .NET Framework 4.8 on Windows Server 2012	4507421 Monthly Rollup 4507412 Security Only	Critical	Remote Code Execution	4499407; 4503866	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2012 (Server Core installation)	4507421 Monthly Rollup 4507412 Security Only	Critical	Remote Code Execution	4499407; 4503866	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 8.1 for 32-bit systems	4507422 Monthly Rollup 4507413 Security Only	Critical	Remote Code Execution	4499408; 4503867	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1113						
Microsoft .NET Framework 4.8 on Windows 8.1 for x64-based systems	4507422 Monthly Rollup 4507413 Security Only	Critical	Remote Code Execution	4499408; 4503867	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2012 R2	4507422 Monthly Rollup 4507413 Security Only	Critical	Remote Code Execution	4499408; 4503867	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows RT 8.1	4507422 Monthly Rollup	Critical	Remote Code Execution	4499408; 4503867	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2012 R2 (Server Core installation)	4507422 Monthly Rollup 4507413 Security Only	Critical	Remote Code Execution	4499408; 4503867	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1113						
Microsoft .NET Framework 4.8 on Windows Server 2016	4506986 Security Update	Critical	Remote Code Execution	4495610; 4502560	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1607 for 32-bit Systems	4506986 Security Update	Critical	Remote Code Execution	4495610; 4502560	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1607 for x64-based Systems	4506986 Security Update	Critical	Remote Code Execution	4495610; 4502560	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2016 (Server Core installation)	4506986 Security Update	Critical	Remote Code Execution	4495610; 4502560	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1703 for 32-bit Systems	4506987 Security Update	Critical	Remote Code Execution	4495611; 4502561	Base: N/A Temporal: N/A	Maybe

CVE-2019-1113						
					Vector: N/A	
Microsoft .NET Framework 4.8 on Windows 10 Version 1703 for x64-based Systems	4506986 Security Update	Critical	Remote Code Execution	4495610; 4502560	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1709 for 32-bit Systems	4506988 Security Update	Critical	Remote Code Execution	4495613; 4502562	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1709 for x64-based Systems	4506986 Security Update	Critical	Remote Code Execution	4495610; 4502560	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1803 for 32-bit Systems	4506989 Security Update	Critical	Remote Code Execution	4495616; 4502563	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1113						
Microsoft .NET Framework 4.8 on Windows 10 Version 1803 for x64-based Systems	4506989 Security Update	Critical	Remote Code Execution	4495616; 4502563	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server, version 1803 (Server Core Installation)	4506989 Security Update	Critical	Remote Code Execution	4495616; 4502563	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Visual Studio 2019 version 16.0	Release Notes Security Update	Critical	Remote Code Execution	4495616; 4502563	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 1809 for 32-bit Systems	4507419 Security Update	Critical	Remote Code Execution	4486553; 4499405; 4503864	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 1809 for x64-based Systems	4507419 Security Update	Critical	Remote Code Execution	4486553; 4499405; 4503864	Base: N/A Temporal: N/A	Maybe

CVE-2019-1113						
					Vector: N/A	
Microsoft .NET Framework 3.5 AND 4.8 on Windows Server 2019	4507419 Security Update	Critical	Remote Code Execution	4486553; 4499405; 4503864	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 AND 4.8 on Windows Server 2019 (Server Core installation)	4507419 Security Update	Critical	Remote Code Execution	4486553; 4499405; 4503864	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 1903 for 32-bit Systems	4506991 Security Update	Critical	Remote Code Execution	4495620; 4502584	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 1903 for x64-based Systems	4506991 Security Update	Critical	Remote Code Execution	4495620; 4502584	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1113						
Microsoft .NET Framework 3.5 AND 4.8 on Windows Server, version 1903 (Server Core installation)	4506991 Security Update	Critical	Remote Code Execution	4495620; 4502584	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 AND 4.7.2 on Windows 10 Version 1809 for 32-bit Systems	4507419 Security Update	Critical	Remote Code Execution	4486553; 4499405; 4503864	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 AND 4.7.2 on Windows 10 Version 1809 for x64-based Systems	4507419 Security Update	Critical	Remote Code Execution	4486553; 4499405; 4503864	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 AND 4.7.2 on Windows Server 2019	4507419 Security Update	Critical	Remote Code Execution	4486553; 4499405; 4503864	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 AND 4.7.2 on Windows Server 2019 (Server Core installation)	4507419 Security Update	Critical	Remote Code Execution	4486553; 4499405; 4503864	Base: N/A Temporal: N/A	Maybe

CVE-2019-1113						
					Vector: N/A	
Microsoft Visual Studio 2019 version 16.1	Release Notes Security Update	Critical	Remote Code Execution	4486553; 4499405; 4503864	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2012	4507412 Security Only 4507421 Monthly Rollup	Critical	Remote Code Execution	4499407; 4503866	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2012 (Server Core installation)	4507412 Security Only 4507421 Monthly Rollup	Critical	Remote Code Execution	4499407; 4503866	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows 8.1 for 32-bit systems	4507413 Security Only 4507422	Critical	Remote Code Execution	4499408; 4503867	Base: N/A Temporal: N/A	Maybe

CVE-2019-1113						
	Monthly Rollup				Vector: N/A	
Microsoft .NET Framework 3.5 on Windows 8.1 for x64-based systems	4507413 Security Only 4507422 Monthly Rollup	Critical	Remote Code Execution	4499408; 4503867	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2012 R2	4507413 Security Only 4507422 Monthly Rollup	Critical	Remote Code Execution	4499408; 4503867	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2012 R2 (Server Core installation)	4507413 Security Only 4507422 Monthly Rollup	Critical	Remote Code Execution	4499408; 4503867	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows 10 for 32-bit Systems	4507458 Security Update	Critical	Remote Code Execution	4503291	Base: N/A Temporal: N/A	Yes

CVE-2019-1113						
					Vector: N/A	
Microsoft .NET Framework 3.5 on Windows 10 for x64-based Systems	4507458 Security Update	Critical	Remote Code Execution	4503291	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows Server 2016	4507460 Security Update	Critical	Remote Code Execution	4503267	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1607 for 32-bit Systems	4507460 Security Update	Critical	Remote Code Execution	4503267	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1607 for x64-based Systems	4507460 Security Update	Critical	Remote Code Execution	4503267	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-1113						
Microsoft .NET Framework 3.5 on Windows Server 2016 (Server Core installation)	4507460 Security Update	Critical	Remote Code Execution	4503267	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1703 for 32-bit Systems	4507450 Security Update	Critical	Remote Code Execution	4503279	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1703 for x64-based Systems	4507450 Security Update	Critical	Remote Code Execution	4503279	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1709 for 32-bit Systems	4507455 Security Update	Critical	Remote Code Execution	4503284	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1709 for x64-based Systems	4507455 Security Update	Critical	Remote Code Execution	4503284	Base: N/A Temporal: N/A	Yes

CVE-2019-1113						
					Vector: N/A	
Microsoft .NET Framework 3.5 on Windows 10 Version 1803 for 32-bit Systems	4507435 Security Update	Critical	Remote Code Execution	4503286	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1803 for x64-based Systems	4507435 Security Update	Critical	Remote Code Execution	4503286	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows Server, version 1803 (Server Core Installation)	4507435 Security Update	Critical	Remote Code Execution	4503286	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for Itanium-Based Systems Service Pack 2	4507414 Security Only 4507423 Monthly Rollup	Critical	Remote Code Execution	4499409; 4503868	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1113						
Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for 32-bit Systems Service Pack 2	4507414 Security Only 4507423 Monthly Rollup	Critical	Remote Code Execution	4499409; 4503868	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for x64-based Systems Service Pack 2	4507414 Security Only 4507423 Monthly Rollup	Critical	Remote Code Execution	4499409; 4503868	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 2.0 Service Pack 2 on Windows Server 2008 for Itanium-Based Systems Service Pack 2	4507414 Security Only 4507423 Monthly Rollup	Critical	Remote Code Execution	4499409; 4503868	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 2.0 Service Pack 2 on Windows Server 2008 for 32-bit Systems Service Pack 2	4507414 Security Only 4507423 Monthly	Critical	Remote Code Execution	4499409; 4503868	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1113						
	Rollup					
Microsoft .NET Framework 2.0 Service Pack 2 on Windows Server 2008 for x64-based Systems Service Pack 2	4507414 Security Only 4507423 Monthly Rollup	Critical	Remote Code Execution	4499409; 4503868	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5.1 on Windows 7 for 32-bit Systems Service Pack 1	4507411 Security Only 4507420 Monthly Rollup	Critical	Remote Code Execution	4499406; 4503865	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5.1 on Windows 7 for x64-based Systems Service Pack 1	4507411 Security Only 4507420 Monthly Rollup	Critical	Remote Code Execution	4499406; 4503865	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4507411 Security Only 4507420	Critical	Remote Code Execution	4499406; 4503865	Base: N/A Temporal: N/A	Maybe

CVE-2019-1113						
	Monthly Rollup				Vector: N/A	
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4507411 Security Only 4507420 Monthly Rollup	Critical	Remote Code Execution	4499406; 4503865	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4507411 Security Only 4507420 Monthly Rollup	Critical	Remote Code Execution	4499406; 4503865	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1116 - Windows GDI Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1116 MITRE NVD	**CVE Title:** Windows GDI Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system. There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document, or by convincing a user to visit an untrusted webpage. The security update addresses the vulnerability by correcting how the Windows GDI component 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 memory layout - the vulnerability allows an attacker to collect information that facilitates predicting addressing of the memory. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1116						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4507449 Monthly Rollup 4507456 Security Only	Important	Information Disclosure	4503292	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	4507449 Monthly Rollup 4507456 Security Only	Important	Information Disclosure	4503292	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	4507449 Monthly Rollup 4507456 Security Only	Important	Information Disclosure	4503292	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-2019-1116						
Core installation)						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4507449 Monthly Rollup 4507456 Security Only	Important	Information Disclosure	4503292	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	4507449 Monthly Rollup 4507456 Security Only	Important	Information Disclosure	4503292	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	4507452 Monthly Rollup 4507461 Security Only	Important	Information Disclosure	4503273	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-2019-1116						
Pack 2 (Server Core installation)						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4507452 Monthly Rollup 4507461 Security Only	Important	Information Disclosure	4503273	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	4507452 Monthly Rollup 4507461 Security Only	Important	Information Disclosure	4503273	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	4507452 Monthly Rollup 4507461	Important	Information Disclosure	4503273	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-2019-1116						
Systems Service Pack 2	Security Only					
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4507452 Monthly Rollup 4507461 Security Only	Important	Information Disclosure	4503273	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-2019-1117 - DirectWrite Remote Code Execution Vulnerability

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
1117 MITRE NVD	A remote code execution vulnerability exists in the way that DirectWrite handles objects in memory. An attacker who successfully exploited this vulnerability 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. There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document, or by convincing a user to visit an untrusted webpage. The security update addresses the vulnerability by correcting how DirectWrite handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1117						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1709 for 32-bit Systems	4507455 Security Update	Important	Remote Code Execution	4503284	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	4507455 Security Update	Important	Remote Code Execution	4503284	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	4507435 Security Update	Important	Remote Code Execution	4503286	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-2019-1117						
Windows 10 Version 1803 for x64-based Systems	4507435 Security Update	Important	Remote Code Execution	4503286	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)	4507435 Security Update	Important	Remote Code Execution	4503286	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	4507435 Security Update	Important	Remote Code Execution	4503286	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	4507469 Security Update	Important	Remote Code Execution	4503327	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-2019-1117						
Windows 10 Version 1809 for x64-based Systems	4507469 Security Update	Important	Remote Code Execution	4503327	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	4507469 Security Update	Important	Remote Code Execution	4503327	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	4507469 Security Update	Important	Remote Code Execution	4503327	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)	4507469 Security Update	Important	Remote Code Execution	4503327	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	4507455 Security Update	Important	Remote Code Execution	4503284	Base: 7.8 Temporal: 7	Yes

CVE-2019-1117						
ARM64-based Systems					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	4507453 Security Update	Important	Remote Code Execution	4503293	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	4507453 Security Update	Important	Remote Code Execution	4503293	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	4507453 Security Update	Important	Remote Code Execution	4503293	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	4507453 Security Update	Important	Remote Code Execution	4503293	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-2019-1117						
(Server Core installation)						

CVE-2019-1118 - DirectWrite Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1118 MITRE NVD	**CVE Title:** DirectWrite Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in the way that DirectWrite handles objects in memory. An attacker who successfully exploited this vulnerability 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. There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document, or by convincing a user to visit an untrusted webpage. The security update addresses the vulnerability by correcting how DirectWrite handles objects in memory.	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1118						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2019-1118						
Windows 10 Version 1709 for 32-bit Systems	4507455 Security Update	Important	Remote Code Execution	4503284	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	4507455 Security Update	Important	Remote Code Execution	4503284	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	4507435 Security Update	Important	Remote Code Execution	4503286	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	4507435 Security Update	Important	Remote Code Execution	4503286	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	4507435 Security Update	Important	Remote Code Execution	4503286	Base: 7.8 Temporal: 7	Yes

CVE-2019-1118						
1803 (Server Core Installation)					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 1803 for ARM64-based Systems	4507435 Security Update	Important	Remote Code Execution	4503286	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	4507469 Security Update	Important	Remote Code Execution	4503327	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	4507469 Security Update	Important	Remote Code Execution	4503327	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	4507469 Security Update	Important	Remote Code Execution	4503327	Base: 7.8 Temporal: 7	Yes

CVE-2019-1118						
ARM64-based Systems					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 2019	4507469 Security Update	Important	Remote Code Execution	4503327	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)	4507469 Security Update	Important	Remote Code Execution	4503327	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 ARM64-based Systems	4507455 Security Update	Important	Remote Code Execution	4503284	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	4507453 Security Update	Important	Remote Code Execution	4503293	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-2019-1118						
Windows 10 Version 1903 for x64-based Systems	4507453 Security Update	Important	Remote Code Execution	4503293	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	4507453 Security Update	Important	Remote Code Execution	4503293	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 (Server Core installation)	4507453 Security Update	Important	Remote Code Execution	4503293	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-2019-1119 - DirectWrite Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1119 MITRE NVD	**CVE Title:** DirectWrite Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in the way that DirectWrite handles objects in memory. An attacker who successfully exploited this vulnerability 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. There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document, or by convincing a user to visit an untrusted webpage. The security update addresses the vulnerability by correcting how DirectWrite handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1119						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1709 for 32-bit Systems	4507455 Security Update	Important	Remote Code Execution	4503284	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-2019-1119						
Windows 10 Version 1709 for x64-based Systems	4507455 Security Update	Important	Remote Code Execution	4503284	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	4507435 Security Update	Important	Remote Code Execution	4503286	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	4507435 Security Update	Important	Remote Code Execution	4503286	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	4507435 Security Update	Important	Remote Code Execution	4503286	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-2019-1119						
Windows 10 Version 1809 for 32-bit Systems	4507469 Security Update	Important	Remote Code Execution	4503327	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	4507469 Security Update	Important	Remote Code Execution	4503327	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	4507469 Security Update	Important	Remote Code Execution	4503327	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	4507469 Security Update	Important	Remote Code Execution	4503327	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	4507469 Security Update	Important	Remote Code Execution	4503327	Base: 7.8 Temporal: 7	Yes

CVE-2019-1119						
Core installation)					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	4507455 Security Update	Important	Remote Code Execution	4503284	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	4507453 Security Update	Important	Remote Code Execution	4503293	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	4507453 Security Update	Important	Remote Code Execution	4503293	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-	4507453 Security Update	Important	Remote Code Execution	4503293	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-2019-1119						
based Systems						

CVE-2019-1120 - DirectWrite Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1120 MITRE NVD	**CVE Title:** DirectWrite Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in the way that DirectWrite handles objects in memory. An attacker who successfully exploited this vulnerability 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. There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document, or by convincing a user to visit an untrusted webpage. The security update addresses the vulnerability by correcting how DirectWrite handles objects in memory.	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1120						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2019-1120						
Windows 10 Version 1709 for 32-bit Systems	4507455 Security Update	Important	Remote Code Execution	4503284	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	4507455 Security Update	Important	Remote Code Execution	4503284	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	4507435 Security Update	Important	Remote Code Execution	4503286	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	4507435 Security Update	Important	Remote Code Execution	4503286	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	4507435 Security Update	Important	Remote Code Execution	4503286	Base: 7.8 Temporal: 7	Yes

CVE-2019-1120						
1803 (Server Core Installation)					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 1803 for ARM64-based Systems	4507435 Security Update	Important	Remote Code Execution	4503286	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	4507469 Security Update	Important	Remote Code Execution	4503327	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	4507469 Security Update	Important	Remote Code Execution	4503327	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	4507469 Security Update	Important	Remote Code Execution	4503327	Base: 7.8 Temporal: 7	Yes

CVE-2019-1120						
ARM64-based Systems					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 2019	4507469 Security Update	Important	Remote Code Execution	4503327	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)	4507469 Security Update	Important	Remote Code Execution	4503327	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 ARM64-based Systems	4507455 Security Update	Important	Remote Code Execution	4503284	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	4507453 Security Update	Important	Remote Code Execution	4503293	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-2019-1120						
Windows 10 Version 1903 for x64-based Systems	4507453 Security Update	Important	Remote Code Execution	4503293	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	4507453 Security Update	Important	Remote Code Execution	4503293	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 (Server Core installation)	4507453 Security Update	Important	Remote Code Execution	4503293	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-2019-1121 - DirectWrite Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1121 MITRE NVD	**CVE Title:** DirectWrite Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in the way that DirectWrite handles objects in memory. An attacker who successfully exploited this vulnerability 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. There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document, or by convincing a user to visit an untrusted webpage. The security update addresses the vulnerability by correcting how DirectWrite handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1121						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1709 for 32-bit Systems	4507455 Security Update	Important	Remote Code Execution	4503284	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-2019-1121						
Windows 10 Version 1709 for x64-based Systems	4507455 Security Update	Important	Remote Code Execution	4503284	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	4507435 Security Update	Important	Remote Code Execution	4503286	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	4507435 Security Update	Important	Remote Code Execution	4503286	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)	4507435 Security Update	Important	Remote Code Execution	4503286	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-2019-1121						
Windows 10 Version 1803 for ARM64-based Systems	4507435 Security Update	Important	Remote Code Execution	4503286	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	4507469 Security Update	Important	Remote Code Execution	4503327	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	4507469 Security Update	Important	Remote Code Execution	4503327	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	4507469 Security Update	Important	Remote Code Execution	4503327	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-2019-1121						
Windows Server 2019	4507469 Security Update	Important	Remote Code Execution	4503327	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)	4507469 Security Update	Important	Remote Code Execution	4503327	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 ARM64-based Systems	4507455 Security Update	Important	Remote Code Execution	4503284	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	4507453 Security Update	Important	Remote Code Execution	4503293	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	4507453 Security Update	Important	Remote Code Execution	4503293	Base: 7.8 Temporal: 7	Yes

CVE-2019-1121						
x64-based Systems					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 ARM64-based Systems	4507453 Security Update	Important	Remote Code Execution	4503293	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 (Server Core installation)	4507453 Security Update	Important	Remote Code Execution	4503293	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-2019-1122 - DirectWrite Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1122 MITRE NVD	**CVE Title:** DirectWrite Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in the way that DirectWrite handles objects in memory. An attacker who successfully exploited this vulnerability 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. There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document, or by convincing a user to visit an untrusted webpage. The security update addresses the vulnerability by correcting how DirectWrite handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1122						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1709 for 32-bit Systems	4507455 Security Update	Important	Remote Code Execution	4503284	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-2019-1122						
Windows 10 Version 1709 for x64-based Systems	4507455 Security Update	Important	Remote Code Execution	4503284	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	4507435 Security Update	Important	Remote Code Execution	4503286	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	4507435 Security Update	Important	Remote Code Execution	4503286	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)	4507435 Security Update	Important	Remote Code Execution	4503286	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-2019-1122						
Windows 10 Version 1803 for ARM64-based Systems	4507435 Security Update	Important	Remote Code Execution	4503286	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	4507469 Security Update	Important	Remote Code Execution	4503327	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	4507469 Security Update	Important	Remote Code Execution	4503327	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	4507469 Security Update	Important	Remote Code Execution	4503327	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-2019-1122						
Windows Server 2019	4507469 Security Update	Important	Remote Code Execution	4503327	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)	4507469 Security Update	Important	Remote Code Execution	4503327	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 ARM64-based Systems	4507455 Security Update	Important	Remote Code Execution	4503284	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	4507453 Security Update	Important	Remote Code Execution	4503293	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	4507453 Security Update	Important	Remote Code Execution	4503293	Base: 7.8 Temporal: 7	Yes

CVE-2019-1122						
x64-based Systems					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 ARM64-based Systems	4507453 Security Update	Important	Remote Code Execution	4503293	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 (Server Core installation)	4507453 Security Update	Important	Remote Code Execution	4503293	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-2019-1123 - DirectWrite Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1123 MITRE NVD	**CVE Title:** DirectWrite Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in the way that DirectWrite handles objects in memory. An attacker who successfully exploited this vulnerability 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. There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document, or by convincing a user to visit an untrusted webpage. The security update addresses the vulnerability by correcting how DirectWrite handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1123						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1709 for 32-bit Systems	4507455 Security Update	Important	Remote Code Execution	4503284	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-2019-1123						
Windows 10 Version 1709 for x64-based Systems	4507455 Security Update	Important	Remote Code Execution	4503284	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	4507435 Security Update	Important	Remote Code Execution	4503286	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	4507435 Security Update	Important	Remote Code Execution	4503286	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)	4507435 Security Update	Important	Remote Code Execution	4503286	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-2019-1123						
Windows 10 Version 1803 for ARM64-based Systems	4507435 Security Update	Important	Remote Code Execution	4503286	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	4507469 Security Update	Important	Remote Code Execution	4503327	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	4507469 Security Update	Important	Remote Code Execution	4503327	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	4507469 Security Update	Important	Remote Code Execution	4503327	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-2019-1123						
Windows Server 2019	4507469 Security Update	Important	Remote Code Execution	4503327	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)	4507469 Security Update	Important	Remote Code Execution	4503327	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 ARM64-based Systems	4507455 Security Update	Important	Remote Code Execution	4503284	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	4507453 Security Update	Important	Remote Code Execution	4503293	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	4507453 Security Update	Important	Remote Code Execution	4503293	Base: 7.8 Temporal: 7	Yes

CVE-2019-1123						
x64-based Systems					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 ARM64-based Systems	4507453 Security Update	Important	Remote Code Execution	4503293	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 (Server Core installation)	4507453 Security Update	Important	Remote Code Execution	4503293	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-2019-1124 - DirectWrite Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1124 MITRE NVD	**CVE Title:** DirectWrite Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in the way that DirectWrite handles objects in memory. An attacker who successfully exploited this vulnerability 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. There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document, or by convincing a user to visit an untrusted webpage. The security update addresses the vulnerability by correcting how DirectWrite handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1124						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1709 for 32-bit Systems	4507455 Security Update	Important	Remote Code Execution	4503284	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-2019-1124						
Windows 10 Version 1709 for x64-based Systems	4507455 Security Update	Important	Remote Code Execution	4503284	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	4507435 Security Update	Important	Remote Code Execution	4503286	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	4507435 Security Update	Important	Remote Code Execution	4503286	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)	4507435 Security Update	Important	Remote Code Execution	4503286	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-2019-1124						
Windows 10 Version 1803 for ARM64-based Systems	4507435 Security Update	Important	Remote Code Execution	4503286	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	4507469 Security Update	Important	Remote Code Execution	4503327	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	4507469 Security Update	Important	Remote Code Execution	4503327	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	4507469 Security Update	Important	Remote Code Execution	4503327	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-2019-1124						
Windows Server 2019	4507469 Security Update	Important	Remote Code Execution	4503327	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)	4507469 Security Update	Important	Remote Code Execution	4503327	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 ARM64-based Systems	4507455 Security Update	Important	Remote Code Execution	4503284	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	4507453 Security Update	Important	Remote Code Execution	4503293	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	4507453 Security Update	Important	Remote Code Execution	4503293	Base: 7.8 Temporal: 7	Yes

CVE-2019-1124						
x64-based Systems					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 ARM64-based Systems	4507453 Security Update	Important	Remote Code Execution	4503293	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 (Server Core installation)	4507453 Security Update	Important	Remote Code Execution	4503293	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-2019-1126 - ADFS Security Feature Bypass Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1126 MITRE NVD	**CVE Title:** ADFS Security Feature Bypass Vulnerability **Description:** A security feature bypass vulnerability exists in Active Directory Federation Services (ADFS) which could allow an attacker to bypass the extranet lockout policy. To exploit this vulnerability, an attacker could run a specially crafted application, which would allow an attacker to launch a password brute-force attack or cause account lockouts in Active Directory. This security update corrects how ADFS handles external authentication requests. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 07/09/2019 07:00:00	Important	Security Feature Bypass

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-2019-1126						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows Server 2012 R2	4507448 Monthly Rollup 4507457 Security Only	Important	Security Feature Bypass	4503276	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4507448 Monthly Rollup 4507457 Security	Important	Security Feature Bypass	4503276	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1126						
	Only					
Windows Server 2016	4507460 Security Update	Important	Security Feature Bypass	4503267	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4507460 Security Update	Important	Security Feature Bypass	4503267	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4507435 Security Update	Important	Security Feature Bypass	4503286	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2019	4507469 Security Update	Important	Security Feature Bypass	4503327	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4507469 Security Update	Important	Security Feature Bypass	4503327	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1126						
Windows Server, version 1903 (Server Core installation)	4507453 Security Update	Important	Security Feature Bypass	4503293	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1127 - DirectWrite Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1127 MITRE NVD	**CVE Title:** DirectWrite Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in the way that DirectWrite handles objects in memory. An attacker who successfully exploited this vulnerability 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. There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document, or by convincing a user to visit an untrusted webpage.	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by correcting how DirectWrite handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1127						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1709 for 32-bit Systems	4507455 Security Update	Important	Remote Code Execution	4503284	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	4507455 Security Update	Important	Remote Code Execution	4503284	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	4507435 Security Update	Important	Remote Code Execution	4503286	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	4507435 Security Update	Important	Remote Code Execution	4503286	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-2019-1127						
Windows Server, version 1803 (Server Core Installation)	4507435 Security Update	Important	Remote Code Execution	4503286	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	4507435 Security Update	Important	Remote Code Execution	4503286	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	4507469 Security Update	Important	Remote Code Execution	4503327	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	4507469 Security Update	Important	Remote Code Execution	4503327	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-2019-1127						
Windows 10 Version 1809 for ARM64-based Systems	4507469 Security Update	Important	Remote Code Execution	4503327	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	4507469 Security Update	Important	Remote Code Execution	4503327	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)	4507469 Security Update	Important	Remote Code Execution	4503327	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 ARM64-based Systems	4507455 Security Update	Important	Remote Code Execution	4503284	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-2019-1127						
Windows 10 Version 1903 for 32-bit Systems	4507453 Security Update	Important	Remote Code Execution	4503293	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	4507453 Security Update	Important	Remote Code Execution	4503293	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	4507453 Security Update	Important	Remote Code Execution	4503293	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 (Server Core installation)	4507453 Security Update	Important	Remote Code Execution	4503293	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-2019-1128 - DirectWrite Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1128 MITRE NVD	**CVE Title:** DirectWrite Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in the way that DirectWrite handles objects in memory. An attacker who successfully exploited this vulnerability 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. There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document, or by convincing a user to visit an untrusted webpage. The security update addresses the vulnerability by correcting how DirectWrite handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1128						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1709 for 32-bit Systems	4507455 Security Update	Important	Remote Code Execution	4503284	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-2019-1128						
Windows 10 Version 1709 for x64-based Systems	4507455 Security Update	Important	Remote Code Execution	4503284	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	4507435 Security Update	Important	Remote Code Execution	4503286	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	4507435 Security Update	Important	Remote Code Execution	4503286	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)	4507435 Security Update	Important	Remote Code Execution	4503286	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-2019-1128						
Windows 10 Version 1803 for ARM64-based Systems	4507435 Security Update	Important	Remote Code Execution	4503286	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	4507469 Security Update	Important	Remote Code Execution	4503327	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	4507469 Security Update	Important	Remote Code Execution	4503327	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	4507469 Security Update	Important	Remote Code Execution	4503327	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-2019-1128						
Windows Server 2019	4507469 Security Update	Important	Remote Code Execution	4503327	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)	4507469 Security Update	Important	Remote Code Execution	4503327	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 ARM64-based Systems	4507455 Security Update	Important	Remote Code Execution	4503284	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	4507453 Security Update	Important	Remote Code Execution	4503293	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	4507453 Security Update	Important	Remote Code Execution	4503293	Base: 7.8 Temporal: 7	Yes

CVE-2019-1128						
x64-based Systems					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 ARM64-based Systems	4507453 Security Update	Important	Remote Code Execution	4503293	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 (Server Core installation)	4507453 Security Update	Important	Remote Code Execution	4503293	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-2019-1129 - Windows Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1129 MITRE NVD	**CVE Title:** Windows Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when Windows AppX Deployment Service (AppXSVC) improperly handles hard links. 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 correcting how Windows AppX Deployment Service handles hard links. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1129						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1703 for 32-bit Systems	4507450 Security Update	Important	Elevation of Privilege	4503279	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	4507450 Security Update	Important	Elevation of Privilege	4503279	Base: 7.8 Temporal: 7	Yes

CVE-2019-1129						
x64-based Systems					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 1709 for 32-bit Systems	4507455 Security Update	Important	Elevation of Privilege	4503284	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	4507455 Security Update	Important	Elevation of Privilege	4503284	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	4507435 Security Update	Important	Elevation of Privilege	4503286	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	4507435 Security Update	Important	Elevation of Privilege	4503286	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	4507435 Security Update	Important	Elevation of Privilege	4503286	Base: 7.8 Temporal: 7	Yes

CVE-2019-1129						
1803 (Server Core Installation)					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 ARM64-based Systems	4507435 Security Update	Important	Elevation of Privilege	4503286	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	4507469 Security Update	Important	Elevation of Privilege	4503327	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	4507469 Security Update	Important	Elevation of Privilege	4503327	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-	4507469 Security Update	Important	Elevation of Privilege	4503327	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-2019-1129						
based Systems						
Windows Server 2019	4507469 Security Update	Important	Elevation of Privilege	4503327	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)	4507469 Security Update	Important	Elevation of Privilege	4503327	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	4507455 Security Update	Important	Elevation of Privilege	4503284	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	4507453 Security Update	Important	Elevation of Privilege	4503293	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	4507453 Security Update	Important	Elevation of Privilege	4503293	Base: 7.8 Temporal: 7	Yes

CVE-2019-1129						
x64-based Systems					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 1903 for ARM64-based Systems	4507453 Security Update	Important	Elevation of Privilege	4503293	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)	4507453 Security Update	Important	Elevation of Privilege	4503293	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-2019-1130 - Windows Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1130 MITRE NVD	**CVE Title:** Windows Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when Windows AppX Deployment Service (AppXSVC) improperly handles hard links. 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 correcting how Windows AppX Deployment Service handles hard links. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1130						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows Server 2012	4507462 Monthly Rollup 4507464 Security Only	Important	Elevation of Privilege	4503285	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-2019-1130						
Windows Server 2012 (Server Core installation)	4507462 Monthly Rollup 4507464 Security Only	Important	Elevation of Privilege	4503285	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	4507448 Monthly Rollup 4507457 Security Only	Important	Elevation of Privilege	4503276	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	4507448 Monthly Rollup 4507457 Security Only	Important	Elevation of Privilege	4503276	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	4507448 Monthly Rollup	Important	Elevation of Privilege	4503276	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-2019-1130						
Windows Server 2012 R2 (Server Core installation)	4507448 Monthly Rollup 4507457 Security Only	Important	Elevation of Privilege	4503276	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	4507458 Security Update	Important	Elevation of Privilege	4503291	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	4507458 Security Update	Important	Elevation of Privilege	4503291	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	4507460 Security Update	Important	Elevation of Privilege	4503267	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	4507460 Security Update	Important	Elevation of Privilege	4503267	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-2019-1130						
Windows 10 Version 1607 for x64-based Systems	4507460 Security Update	Important	Elevation of Privilege	4503267	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)	4507460 Security Update	Important	Elevation of Privilege	4503267	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	4507450 Security Update	Important	Elevation of Privilege	4503279	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	4507450 Security Update	Important	Elevation of Privilege	4503279	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	4507455 Security Update	Important	Elevation of Privilege	4503284	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-2019-1130						
Windows 10 Version 1709 for x64-based Systems	4507455 Security Update	Important	Elevation of Privilege	4503284	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	4507435 Security Update	Important	Elevation of Privilege	4503286	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	4507435 Security Update	Important	Elevation of Privilege	4503286	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)	4507435 Security Update	Important	Elevation of Privilege	4503286	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	4507435 Security Update	Important	Elevation of Privilege	4503286	Base: 7.8 Temporal: 7	Yes

CVE-2019-1130						
ARM64-based Systems					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 1809 for 32-bit Systems	4507469 Security Update	Important	Elevation of Privilege	4503327	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	4507469 Security Update	Important	Elevation of Privilege	4503327	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	4507469 Security Update	Important	Elevation of Privilege	4503327	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	4507469 Security Update	Important	Elevation of Privilege	4503327	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-2019-1130						
Windows Server 2019 (Server Core installation)	4507469 Security Update	Important	Elevation of Privilege	4503327	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	4507455 Security Update	Important	Elevation of Privilege	4503284	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	4507453 Security Update	Important	Elevation of Privilege	4503293	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	4507453 Security Update	Important	Elevation of Privilege	4503293	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-	4507453 Security Update	Important	Elevation of Privilege	4503293	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-2019-1130						
based Systems						
Windows Server, version 1903 (Server Core installation)	4507453 Security Update	Important	Elevation of Privilege	4503293	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-2019-1132 - Win32k Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1132 MITRE NVD	**CVE Title:** Win32k Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in Windows when the Win32k component 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.	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 update addresses this vulnerability by correcting how Win32k handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1132						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4507449 Monthly Rollup 4507456 Security Only	Important	Elevation of Privilege	4503292	Base: 7.8 Temporal: 7.2 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4507449 Monthly Rollup 4507456 Security Only	Important	Elevation of Privilege	4503292	Base: 7.8 Temporal: 7.2 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4507449 Monthly Rollup 4507456 Security Only	Important	Elevation of Privilege	4503292	Base: 7.8 Temporal: 7.2 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Yes

CVE-2019-1132						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4507449 Monthly Rollup 4507456 Security Only	Important	Elevation of Privilege	4503292	Base: 7.8 Temporal: 7.2 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4507449 Monthly Rollup 4507456 Security Only	Important	Elevation of Privilege	4503292	Base: 7.8 Temporal: 7.2 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4507452 Monthly Rollup 4507461 Security Only	Important	Elevation of Privilege	4503273	Base: 7.8 Temporal: 7.2 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Yes

CVE-2019-1132						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4507452 Monthly Rollup 4507461 Security Only	Important	Elevation of Privilege	4503273	Base: 7.8 Temporal: 7.2 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4507452 Monthly Rollup 4507461 Security Only	Important	Elevation of Privilege	4503273	Base: 7.8 Temporal: 7.2 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4507452 Monthly Rollup 4507461 Security Only	Important	Elevation of Privilege	4503273	Base: 7.8 Temporal: 7.2 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Yes
Windows Server 2008 for x64-	4507452 Monthly Rollup	Important	Elevation of Privilege	4503273	Base: 7.8 Temporal: 7.2	Yes

CVE-2019-1132						
based Systems Service Pack 2 (Server Core installation)	4507461 Security Only				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	

CVE-2019-1134 - Microsoft Office SharePoint XSS Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1134 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. 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	Important	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1134						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SharePoint Enterprise Server 2016	4475520 Security Update	Important	Spoofing	4464594	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Enterprise Server 2013 Service Pack 1	4475522 Security Update	Important	Spoofing	4464597	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Server 2019	4475529 Security Update	Important	Spoofing	4475512	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1136 - Microsoft Exchange Server Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1136 MITRE NVD	**CVE Title:** Microsoft Exchange Server Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in Microsoft Exchange Server. An attacker who successfully exploited this vulnerability could gain the same rights as any other user of the Exchange server. This could allow the attacker to perform activities such as accessing the mailboxes of other users. Exploitation of this vulnerability requires Exchange Web Services (EWS) to be enabled and in use in an affected environment. To exploit the vulnerability, an attacker would need to execute a man-in-the-middle attack to forward an authentication request to a Microsoft Exchange Server, thereby allowing impersonation of another Exchange user. To address this vulnerability, Microsoft has changed the way EWS handles NTLM tokens. **FAQ:** None	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1136						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Exchange Server 2010 Service Pack 3	4509410 Security Update	Important	Elevation of Privilege	4503028	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1136						
Microsoft Exchange Server 2016 Cumulative Update 12	4509409 Security Update	Important	Elevation of Privilege	4503027	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Exchange Server 2016 Cumulative Update 13	4509409 Security Update	Important	Elevation of Privilege	4503027	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Exchange Server 2013 Cumulative Update 23	4509409 Security Update	Important	Elevation of Privilege	4503027	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1137 - Microsoft Exchange Server Spoofing Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1137	**CVE Title:** Microsoft Exchange Server Spoofing Vulnerability **Description:**	Important	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	A cross-site-scripting (XSS) vulnerability exists when Microsoft Exchange Server does not properly sanitize a specially crafted web request to an affected Exchange server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected 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. 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 Exchange 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 Exchange Server properly sanitizes web requests. **FAQ:** None **Mitigations:** None **Workarounds:** None		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 07/09/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1137						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Exchange Server 2016 Cumulative Update 12	4509409 Security Update	Important	Spoofing	4503027	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Exchange Server 2019 Cumulative Update 1	4509408 Security Update	Important	Spoofing	4503027	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1137						
Microsoft Exchange Server 2019 Cumulative Update 2	4509408 Security Update	Important	Spoofing	4503027	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Exchange Server 2016 Cumulative Update 13	4509409 Security Update	Important	Spoofing	4503027	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Exchange Server 2013 Cumulative Update 23	4509409 Security Update	Important	Spoofing	4503027	Base: N/A Temporal: N/A Vector: N/A	Maybe

声 明

==========

本安全公告仅用来描述可能存在的安全问题，绿盟科技不为此安全公告提供任何保证或承诺。由于传播、利用此安全公告所提供的信息而造成的任何直接或者间接的后果及损失，均由使用者本人负责，绿盟科技以及安全公告作者不为此承担任何责任。绿盟科技拥有对此安全公告的修改和解释权。如欲转载或传播此安全公告，必须保证此安全公告的完整性，包括版权声明等全部内容。未经绿盟科技允许，不得任意修改或者增减此安全公告内容，不得以任何方式将其用于商业目的。

关于绿盟科技

==========

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