微软发布 9 月补丁修复 83 个安全问题

安全威胁通告

发布时间：2017 年 9 月 13 日

综述

微软于周二发布了 9 月安全更新补丁，修复了 83 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 Internet Explorer、Microsoft Edge、.NET Framework、Microsoft Windows、Microsoft Office、Microsoft Windows PDF、Windows Hyper-V 以及 Adobe Flash Player。

相关信息如下（红色部分威胁相对比较高）：

产品	CVE 编号	CVE 标题
.NET Framework	CVE-2017-8759	.NET Framework 远程代码执行漏洞

Adobe Flash Player	ADV170013	2017 年 9 月 Flash 安全更新
Device Guard	CVE-2017-8746	Device Guard 安全功能绕过漏洞
HoloLens	CVE-2017-9417	博通 BCM43xx 远程代码执行漏洞
Internet Explorer	CVE-2017-8749	Internet 浏览器内存损坏漏洞
Internet Explorer	CVE-2017-8747	Internet 浏览器内存损坏漏洞
Internet Explorer	CVE-2017-8733	Internet 浏览器欺骗性漏洞
Microsoft Bluetooth Driver	CVE-2017-8628	Microsoft 蓝牙驱动欺骗性漏洞
Microsoft Browsers	CVE-2017-8736	Microsoft 浏览器信息泄露漏洞

Microsoft Browsers	CVE-2017-8750	Microsoft 浏览器内存破坏漏洞
Microsoft Edge	CVE-2017-8757	Microsoft Edge 远程代码执行漏洞
Microsoft Edge	CVE-2017-8597	Microsoft Edge 信息泄露漏洞
Microsoft Edge	CVE-2017-8723	Microsoft Edge 安全功能绕过漏洞
Microsoft Edge	CVE-2017-11766	Microsoft Edge 内存破坏漏洞
Microsoft Edge	CVE-2017-8643	Microsoft Edge 信息泄露漏洞
Microsoft Edge	CVE-2017-8648	Microsoft Edge 信息泄露漏洞
Microsoft Edge	CVE-2017-8735	Microsoft Edge 欺骗漏洞

Microsoft Edge	CVE-2017-8755	Scripting Engine 内存破坏漏洞
Microsoft Edge	CVE-2017-8754	Microsoft Edge 安全功能绕过漏洞
Microsoft Edge	CVE-2017-8751	Microsoft Edge 内存破坏漏洞
Microsoft Edge	CVE-2017-8734	Microsoft Edge 内存破坏漏洞
Microsoft Edge	CVE-2017-8724	Microsoft Edge 欺骗漏洞
Microsoft Edge	CVE-2017-8731	Microsoft Edge 内存破坏漏洞
Microsoft Edge	CVE-2017-8756	Scripting Engine 内存破坏漏洞
Microsoft Exchange Server	CVE-2017-11761	Microsoft Exchange 信息泄露漏洞

Microsoft Exchange Server	CVE-2017-8758	Microsoft Exchange 跨站脚本漏洞
Microsoft Graphics Component	CVE-2017-8688	Windows GDI+ 信息泄露漏洞
Microsoft Graphics Component	CVE-2017-8685	Windows GDI+ 信息泄露漏洞
Microsoft Graphics Component	CVE-2017-8695	图形组件信息泄露漏洞
Microsoft Graphics Component	CVE-2017-8683	Win32k Graphics 信息泄露漏洞
Microsoft Graphics Component	CVE-2017-8696	Microsoft Graphics Component 远程代码执行漏洞
Microsoft Graphics Component	CVE-2017-8684	Windows GDI+ 信息泄露漏洞

Microsoft Graphics Component	CVE-2017-8682	Win32k Graphics 远程代码执行漏洞
Microsoft Graphics Component	CVE-2017-8720	Win32k 特权提升漏洞
Microsoft Graphics Component	CVE-2017-8676	Windows GDI+ 信息泄露漏洞
Microsoft Office	CVE-2017-8632	Microsoft Office 内存破坏漏洞
Microsoft Office	CVE-2017-8725	Microsoft Office Publisher 远程代码执行漏洞
Microsoft Office	CVE-2017-8630	Microsoft Office 内存破坏漏洞
Microsoft Office	CVE-2017-8743	PowerPoint 远程代码执行漏洞
Microsoft Office	CVE-2017-8742	PowerPoint 远程代码执行漏洞

Microsoft Office	CVE-2017-8745	Microsoft SharePoint 跨站脚本漏洞
Microsoft Office	CVE-2017-8744	Microsoft Office 内存破坏漏洞
Microsoft Office	CVE-2017-8567	Microsoft Office 远程代码执行漏洞
Microsoft Office	ADV170015	Microsoft Office Defense 深度更新
Microsoft Office	CVE-2017-8629	Microsoft SharePoint XSS 漏洞
Microsoft Office	CVE-2017-8631	Microsoft Office 内存破坏漏洞
Microsoft Scripting Engine	CVE-2017-8738	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine	CVE-2017-8729	Scripting Engine 内存破坏漏洞

Microsoft Scripting Engine	CVE-2017-8739	Scripting Engine 信息泄露漏洞
Microsoft Scripting Engine	CVE-2017-8740	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine	CVE-2017-8741	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine	CVE-2017-8649	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine	CVE-2017-8660	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine	CVE-2017-8748	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine	CVE-2017-11764	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine	CVE-2017-8752	Scripting Engine 内存破坏漏洞

Microsoft Scripting Engine	CVE-2017-8753	Scripting Engine 内存破坏漏洞
Microsoft Uniscribe	CVE-2017-8692	Uniscribe 远程代码执行漏洞
Microsoft Windows	CVE-2017-8699	Windows Shell 远程代码执行漏洞
Microsoft Windows	CVE-2017-8710	Windows 信息泄露漏洞
Microsoft Windows	CVE-2017-8716	Windows 安全功能绕过漏洞
Microsoft Windows	CVE-2017-8702	Windows 特权提升漏洞
Microsoft Windows PDF	CVE-2017-8737	Microsoft PDF 远程代码执行漏洞
Microsoft Windows PDF	CVE-2017-8728	Microsoft PDF 远程代码执行漏洞

Windows DHCP Server	CVE-2017-8686	Windows DHCP Server 远程代码执行漏洞
Windows Hyper-V	CVE-2017-8712	Hyper-V 信息泄露漏洞
Windows Hyper-V	CVE-2017-8713	Hyper-V 信息泄露漏洞
Windows Hyper-V	CVE-2017-8714	Remote Desktop Virtual Host 远程代码执行漏洞
Windows Hyper-V	CVE-2017-8711	Hyper-V 信息泄露漏洞
Windows Hyper-V	CVE-2017-8707	Hyper-V 信息泄露漏洞
Windows Hyper-V	CVE-2017-8704	Hyper-V 拒绝服务漏洞
Windows Hyper-V	CVE-2017-8706	Hyper-V 信息泄露漏洞

Windows Kernel	CVE-2017-8719	Windows 内核信息泄露漏洞
Windows Kernel	CVE-2017-8708	Windows 内核信息泄露漏洞
Windows Kernel	CVE-2017-8679	Windows 内核信息泄露漏洞
Windows Kernel	CVE-2017-8709	Windows 内核信息泄露漏洞
Windows Kernel-Mode Drivers	CVE-2017-8687	Win32k 信息泄露漏洞
Windows Kernel-Mode Drivers	CVE-2017-8681	Win32k 信息泄露漏洞
Windows Kernel-Mode Drivers	CVE-2017-8675	Win32k 权限提升漏洞
Windows Kernel-Mode Drivers	CVE-2017-8678	Win32k 信息泄露漏洞

Windows Kernel-Mode Drivers	CVE-2017-8677	Win32k 信息泄露漏洞
Windows Kernel-Mode Drivers	CVE-2017-8680	Win32k 信息泄露漏洞
Windows NetBIOS	CVE-2017-0161	NetBIOS 远程代码执行漏洞

受影响的状况

见附件部分。

CVE-2017-8597 - Microsoft Edge Information Disclosure Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8597 MITRE NVD	**CVE Title:** Microsoft Edge Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when Microsoft Edge does not properly handle objects in memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the user's system. In a web-based attack scenario, an attacker could host a website in an attempt to exploit the vulnerability. In addition, compromised websites and websites that accept or host user-provided content could contain specially crafted content that could exploit the vulnerability. However, in all cases an attacker would have no way to force a user to view the attacker-controlled content. Instead, an attacker would have to convince a user to take action. For example, an attacker could trick a user into clicking a link that takes the user to the attacker's site. The security update addresses the vulnerability by changing how Microsoft Edge handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8597						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4038788 (Security Update)	Important	Information Disclosure	4034674	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8597						
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4038788 (Security Update)	Important	Information Disclosure	4034674	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8629 - Microsoft SharePoint XSS Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8629	**CVE Title:** Microsoft SharePoint XSS Vulnerability **Description:** An elevation of privilege vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. These attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8629						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SharePoint Server 2013 Service Pack 1	4011113 (Security Update)	Important	Elevation of Privilege	3203387	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-8630 - Microsoft Office Memory Corruption Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8630	**CVE Title:** Microsoft Office Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in Microsoft Office software when it fails to properly handle objects in memory. An attacker who successfully exploited the	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	vulnerability could use a specially crafted file to perform actions in the security context of the current user. For example, the file could then take actions on behalf of the logged-on user with the same permissions as the current user. Exploitation of this vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Office software. 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) that contains a specially crafted file that is designed to exploit the vulnerability. However, an attacker would have no way to force the user to visit the website. Instead, an attacker would have to convince the user to click a link, typically by way of an enticement in an email or Instant Messenger message, and then convince the user to open the specially crafted file. The security update addresses the vulnerability by correcting how Microsoft Office handles files in memory. **FAQ:** None **Mitigations:** None **Workarounds:**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8630						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Office 2016 (32-bit edition)	3203474 (Security Update)	Important	Remote Code Execution	None	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 (64-bit edition)	3203474 (Security Update)	Important	Remote Code Execution	None	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-8631 - Microsoft Office Memory Corruption Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8631 MITRE NVD	**CVE Title:** Microsoft Office Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in Microsoft Office software when it fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could use a specially crafted file to perform actions in the security context of the current user. For example, the file could then take actions on behalf of the logged-on user with the same permissions as the current user. Exploitation of this vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Office software. 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) that contains a specially crafted file that is designed to exploit the vulnerability. However, an attacker would have no way to force the user to visit the website. Instead, an attacker would have to convince the user to click a link, typically by way of an enticement in an email or Instant Messenger message, and then convince the user to open the specially crafted file.	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by correcting how Microsoft Office handles files in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8631						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2017-8631						
Excel Services on Microsoft SharePoint Server 2007 Service Pack 3 (32-bit editions)	3191831 (Security Update)	Important	Remote Code Execution	3178678	Base: N/A Temporal: N/A Vector: N/A	Maybe
Excel Services on Microsoft SharePoint Server 2007 Service Pack 3 (64-bit editions)	3191831 (Security Update)	Important	Remote Code Execution	3178678	Base: N/A Temporal: N/A Vector: N/A	Maybe
Excel Services on Microsoft SharePoint Server 2010 Service Pack 2	4011056 (Security Update)	Important	Remote Code Execution	3191902	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2007 Service Pack 3	4011062 (Security Update)	Important	Remote Code Execution	None	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2010 Service Pack 2 (32-bit editions)	4011061 (Security Update)	Important	Remote Code Execution	3191907	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2010 Service Pack 2 (64-bit editions)	4011061 (Security Update)	Important	Remote Code Execution	3191907	Base: N/A Temporal:	Maybe

CVE-2017-8631						
					N/A Vector: N/A	
Microsoft Excel 2013 RT Service Pack 1	4011108 (Security Update)	Important	Remote Code Execution	3213537	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2013 Service Pack 1 (32-bit editions)	4011108 (Security Update)	Important	Remote Code Execution	None	Base: N/A Temporal: N/A Vector: N/A	Unknown
Microsoft Excel 2013 Service Pack 1 (64-bit editions)	4011108 (Security Update)	Important	Remote Code Execution	None	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2016 (32-bit edition)	4011050 (Security Update)	Important	Remote Code Execution	3203477	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2016 (64-bit edition)	4011050 (Security Update)	Important	Remote Code Execution	3203477	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-8631						
Microsoft Excel 2016 for Mac	Release Notes (Security Update)	Important	Remote Code Execution	None	Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Excel for Mac 2011	3212225 (Security Update)	Important	Remote Code Execution	None	Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Excel Viewer 2007 Service Pack 3	4011065 (Security Update)	Important	Remote Code Execution	None	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel Web App 2013 Service Pack 1	3213562 (Security Update)	Important	Remote Code Execution	None	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office Compatibility Pack Service Pack 3	4011064 (Security Update)	Important	Remote Code Execution	None	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office Web Apps 2013 Service Pack 1	3213562 (Security Update)	Important	Remote Code Execution	None	Base: N/A Temporal:	Maybe

CVE-2017-8631						
					N/A Vector: N/A	
Office Online Server	3213658 (Security Update)	Important	Remote Code Execution	None	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-8632 - Microsoft Office Memory Corruption Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8632 MITRE NVD	**CVE Title:** Microsoft Office Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in Microsoft Office software when it fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could use a specially crafted file to perform actions in the security context of the current user. For example, the file could then take actions on behalf of the logged-on user with the same permissions as the current user. Exploitation of this	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Office software. 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) that contains a specially crafted file that is designed to exploit the vulnerability. However, an attacker would have no way to force the user to visit the website. Instead, an attacker would have to convince the user to click a link, typically by way of an enticement in an email or Instant Messenger message, and then convince the user to open the specially crafted file. The security update addresses the vulnerability by correcting how Microsoft Office handles files in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8632						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Excel 2010 Service Pack 2 (32-bit editions)	4011061 (Security Update)	Important	Remote Code Execution	3191907	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2010 Service Pack 2 (64-bit editions)	4011061 (Security Update)	Important	Remote Code Execution	3191907	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2013 RT Service Pack 1	4011108 (Security Update)	Important	Remote Code Execution	3213537	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2013 Service Pack 1 (32-bit editions)	4011108 (Security Update)	Important	Remote Code Execution	3213537	Base: N/A Temporal:	Maybe

CVE-2017-8632						
					N/A Vector: N/A	
Microsoft Excel 2013 Service Pack 1 (64-bit editions)	4011108 (Security Update)	Important	Remote Code Execution	3213537	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2016 (32-bit edition)	4011050 (Security Update)	Important	Remote Code Execution	3203477	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2016 (64-bit edition)	4011050 (Security Update)	Important	Remote Code Execution	3203477	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2016 for Mac	Release Notes (Security Update)	Important	Remote Code Execution	None	Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Excel for Mac 2011	3212225 (Security Update)	Important	Remote Code Execution	None	Base: N/A Temporal: N/A Vector: N/A	No

CVE-2017-8632						
Microsoft Office Compatibility Pack Service Pack 3	4011064 (Security Update)	Important	Remote Code Execution	None	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-8675 - Win32k Elevation of Privilege Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8675 MITRE NVD	**CVE Title:** Win32k Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The update addresses this vulnerability by correcting how the Windows kernel-mode driver handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8675						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2017-8675						
Windows 10 for 32-bit Systems	4038781 (Security Update)	Important	Elevation of Privilege	4034668	Base: 7.00 Temporal: 6.30 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	4038781 (Security Update)	Important	Elevation of Privilege	4034668	Base: 7.00 Temporal: 6.30 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 1511 for 32-bit Systems	4038783 (Security Update)	Important	Elevation of Privilege	4034660	Base: 7.00 Temporal: 6.30 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 1511 for x64-based Systems	4038783 (Security Update)	Important	Elevation of Privilege	4034660	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4038782 (Security Update)	Important	Elevation of Privilege	4034658	Base: 7.00 Temporal: 6.30 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-2017-8675						
Windows 10 Version 1607 for x64-based Systems	4038782 (Security Update)	Important	Elevation of Privilege	4034658	Base: 7.00 Temporal: 6.30 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	4038788 (Security Update)	Important	Elevation of Privilege	4034674	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4038788 (Security Update)	Important	Elevation of Privilege	4034674	Base: 7.00 Temporal: 6.30 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 7 for 32-bit Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Elevation of Privilege	4034664	Base: 7.00 Temporal: 6.30 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-2017-8675						
Windows 7 for x64-based Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Elevation of Privilege	4034664	Base: 7.00 Temporal: 6.30 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	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Elevation of Privilege	4034681	Base: 7.00 Temporal: 6.30 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	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Elevation of Privilege	4034681	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4038792 (Monthly Rollup)	Important	Elevation of Privilege	4034681	Base: 7.00 Temporal: 6.30 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-2017-8675						
Windows Server 2008 for 32-bit Systems Service Pack 2	4039384 (Security Update)	Important	Elevation of Privilege	4022887	Base: 7.00 Temporal: 6.30 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	Unknown
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4039384 (Security Update)	Important	Elevation of Privilege	4022887	Base: 7.00 Temporal: 6.30 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	Unknown
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4039384 (Security Update)	Important	Elevation of Privilege	4022887	Base: 7.00 Temporal: 6.30 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	Unknown

CVE-2017-8675						
Windows Server 2008 for x64-based Systems Service Pack 2	4039384 (Security Update)	Important	Elevation of Privilege	4022887	Base: 7.00 Temporal: 6.30 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	Unknown
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4039384 (Security Update)	Important	Elevation of Privilege	4022887	Base: 7.00 Temporal: 6.30 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	Unknown
Windows Server 2008 R2 for Itanium-Based Systems	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Elevation of Privilege	4034664	Base: 7.00 Temporal: 6.30 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-2017-8675						
Service Pack 1						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Elevation of Privilege	4034664	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Elevation of Privilege	4034664	Base: 7.00 Temporal: 6.30 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	4038786 (Security Only) 4038799	Important	Elevation of Privilege	4034665	Base: 7.00 Temporal: 6.30 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-2017-8675						
	(Monthly Rollup)					
Windows Server 2012 (Server Core installation)	4038786 (Security Only) 4038799 (Monthly Rollup)	Important	Elevation of Privilege	4034665	Base: 7.00 Temporal: 6.30 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	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Elevation of Privilege	4034681	Base: 7.00 Temporal: 6.30 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)	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Elevation of Privilege	4034681	Base: 7.00 Temporal: 6.30 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	4038782 (Security Update)	Important	Elevation of Privilege	4034658	Base: 7.00 Temporal: 6.30	Yes

CVE-2017-8675						
					Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2016 (Server Core installation)	4038782 (Security Update)	Important	Elevation of Privilege	4034658	Base: 7.00 Temporal: 6.30 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-2017-8676 - Windows GDI+ Information Disclosure Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8676 MITRE NVD	**CVE Title:** Windows GDI+ Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, allowing an attacker to retrieve information from a targeted system. By itself, the information disclosure does not allow	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	arbitrary code execution; however, it could allow arbitrary code to be run if the attacker uses it in combination with another vulnerability. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. Note that where the severity is indicated as Critical in the Affected Products table, the Preview Pane is an attack vector for this vulnerability. The security update addresses the vulnerability by correcting how GDI handles memory addresses. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8676						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Live Meeting 2007 Add-in	4025869 (Security Update)	Important	Information Disclosure	4020736	Base: N/A Temporal: N/A Vector: N/A	Unknown
Microsoft Live Meeting 2007 Console	4025868 (Security Update)	Important	Information Disclosure	4020735	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Lync 2010 (32-bit)	4025865 (Security Update)	Important	Information Disclosure	4020732	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Lync 2010 (64-bit)	4025865 (Security Update)	Important	Information Disclosure	4020732	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-8676						
Microsoft Lync 2010 Attendee (admin level install)	4025866 (Security Update)	Important	Information Disclosure	4020733	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Lync 2010 Attendee (user level install)	4025867 (Security Update)	Important	Information Disclosure	4020734	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Lync 2013 Service Pack 1 (32-bit)	4011107 (Security Update)	Important	Information Disclosure	3191939	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Lync 2013 Service Pack 1 (64-bit)	4011107 (Security Update)	Important	Information Disclosure	3191939	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-8676						
Microsoft Lync Basic 2013 Service Pack 1 (32-bit)	4011107 (Security Update)	Important	Information Disclosure	3191939	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Lync Basic 2013 Service Pack 1 (64-bit)	4011107 (Security Update)	Important	Information Disclosure	3191939	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2007 Service Pack 3	3213641 (Security Update)	Important	Information Disclosure	None	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (32-bit editions)	3213638 (Security Update)	Important	Information Disclosure	3191848	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-8676						
Microsoft Office 2010 Service Pack 2 (64-bit editions)	3213638 (Security Update)	Important	Information Disclosure	3191848	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 for Mac	Release Notes (Security Update)	Important	Information Disclosure	None	Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Office for Mac 2011	3212225 (Security Update)	Important	Information Disclosure	None	Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Office Word Viewer	4011134 (Security Update)	Critical	Information Disclosure	3203484	Base: N/A Temporal: N/A Vector: N/A	Maybe
Skype for Business 2016 (32-bit)	4011040 (Security Update)	Important	Information Disclosure	3203382	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-8676						
Skype for Business 2016 (64-bit)	4011040 (Security Update)	Important	Information Disclosure	3203382	Base: N/A Temporal: N/A Vector: N/A	Maybe
Skype for Business 2016 Basic (32-bit)	4011040 (Security Update)	Important	Information Disclosure	3203382	Base: N/A Temporal: N/A Vector: N/A	Maybe
Skype for Business 2016 Basic (64-bit)	4011040 (Security Update)	Important	Information Disclosure	3203382	Base: N/A Temporal: N/A Vector: N/A	Maybe
Windows 10 for 32-bit Systems	4038781 (Security Update)	Important	Information Disclosure	4034668	Base: 3.30 Temporal: 3.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4038781 (Security Update)	Important	Information Disclosure	4034668	Base: 3.30 Temporal: 3.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for	4038783 (Security Update)	Important	Information Disclosure	4034660	Base: 3.30 Temporal: 3.00	Yes

CVE-2017-8676						
32-bit Systems					Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1511 for x64-based Systems	4038783 (Security Update)	Important	Information Disclosure	4034660	Base: 3.30 Temporal: 3.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 3.30 Temporal: 3.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 3.30 Temporal: 3.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4038788 (Security Update)	Important	Information Disclosure	4034674	Base: 3.30 Temporal: 3.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8676						
Windows 10 Version 1703 for x64-based Systems	4038788 (Security Update)	Important	Information Disclosure	4034674	Base: 3.30 Temporal: 3.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 7 for 32-bit Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 3.30 Temporal: 3.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 3.30 Temporal: 3.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Information Disclosure	4034681	Base: 3.30 Temporal: 3.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8676						
Windows 8.1 for x64-based systems	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Information Disclosure	4034681	Base: 3.30 Temporal: 3.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4038792 (Monthly Rollup)	Important	Information Disclosure	4034681	Base: 3.30 Temporal: 3.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4039384 (Security Update)	Important	Information Disclosure	4022887	Base: 3.30 Temporal: 3.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for 32-bit Systems Service	4039384 (Security Update)	Important	Information Disclosure	4022887	Base: 3.30 Temporal: 3.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Unknown

CVE-2017-8676						
Pack 2 (Server Core installation)						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4039384 (Security Update)	Important	Information Disclosure	4022887	Base: 3.30 Temporal: 3.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for x64-based Systems Service Pack 2	4039384 (Security Update)	Important	Information Disclosure	4022887	Base: 3.30 Temporal: 3.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for x64-based	4039384 (Security Update)	Important	Information Disclosure	4022887	Base: 3.30 Temporal: 3.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Unknown

CVE-2017-8676						
Systems Service Pack 2 (Server Core installation)						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 3.30 Temporal: 3.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 3.30 Temporal: 3.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server	4038777 (Monthly	Important	Information Disclosure	4034664	Base: 3.30 Temporal: 3.00	Yes

CVE-2017-8676						
2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	Rollup) 4038779 (Security Only)				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2012	4038786 (Security Only) 4038799 (Monthly Rollup)	Important	Information Disclosure	4034665	Base: 3.30 Temporal: 3.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4038786 (Security Only) 4038799 (Monthly Rollup)	Important	Information Disclosure	4034665	Base: 3.30 Temporal: 3.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4038792 (Monthly Rollup)	Important	Information Disclosure	4034681	Base: 3.30 Temporal: 3.00	Yes

CVE-2017-8676						
	4038793 (Security Only)				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2012 R2 (Server Core installation)	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Information Disclosure	4034681	Base: 3.30 Temporal: 3.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 3.30 Temporal: 3.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 3.30 Temporal: 3.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8677 - Win32k Information Disclosure Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8677 MITRE NVD	**CVE Title:** Win32k Information Disclosure Vulnerability **Description:** A information disclosure vulnerability exists when the Windows GDI+ component improperly discloses kernel memory addresses. An attacker who successfully exploited the vulnerability could obtain information to further compromise the user'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 security update addresses the vulnerability by correcting how the Windows GDI+ component handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8677						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	4038781 (Security Update)	Important	Information Disclosure	4034668	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8677						
Windows 10 for x64-based Systems	4038781 (Security Update)	Important	Information Disclosure	4034668	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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 1511 for 32-bit Systems	4038783 (Security Update)	Important	Information Disclosure	4034660	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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 1511 for x64-based Systems	4038783 (Security Update)	Important	Information Disclosure	4034660	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 5.50 Temporal: 5.00 Vector:	Yes

CVE-2017-8677						
x64-based Systems					CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1703 for 32-bit Systems	4038788 (Security Update)	Important	Information Disclosure	4034674	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038788 (Security Update)	Important	Information Disclosure	4034674	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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 32-bit Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038777 (Monthly Rollup) 4038779	Important	Information Disclosure	4034664	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8677						
Service Pack 1	(Security Only)					
Windows 8.1 for 32-bit systems	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Information Disclosure	4034681	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Information Disclosure	4034681	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038792 (Monthly Rollup)	Important	Information Disclosure	4034681	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038777 (Monthly Rollup) 4038779	Important	Information Disclosure	4034664	Base: 5.50 Temporal: 5.00 Vector:	Yes

CVE-2017-8677						
Itanium-Based Systems Service Pack 1	(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	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8677						
installation)						
Windows Server 2012	4038786 (Security Only) 4038799 (Monthly Rollup)	Important	Information Disclosure	4034665	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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)	4038786 (Security Only) 4038799 (Monthly Rollup)	Important	Information Disclosure	4034665	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Information Disclosure	4034681	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8677						
Windows Server 2012 R2 (Server Core installation)	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Information Disclosure	4034681	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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)	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8678 - Win32k Information Disclosure Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8678 MITRE NVD	**CVE Title:** Win32k 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 user'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:** None **Mitigations:** None **Workarounds:**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8678						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	4038781 (Security Update)	Important	Information Disclosure	4034668	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8678						
Windows 10 for x64-based Systems	4038781 (Security Update)	Important	Information Disclosure	4034668	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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 1511 for 32-bit Systems	4038783 (Security Update)	Important	Information Disclosure	4034660	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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 1511 for x64-based Systems	4038783 (Security Update)	Important	Information Disclosure	4034660	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 5.50 Temporal: 5.00 Vector:	Yes

CVE-2017-8678						
x64-based Systems					CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1703 for 32-bit Systems	4038788 (Security Update)	Important	Information Disclosure	4034674	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038788 (Security Update)	Important	Information Disclosure	4034674	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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 32-bit Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038777 (Monthly Rollup) 4038779	Important	Information Disclosure	4034664	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8678						
Service Pack 1	(Security Only)					
Windows 8.1 for 32-bit systems	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Information Disclosure	4034681	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Information Disclosure	4034681	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038792 (Monthly Rollup)	Important	Information Disclosure	4034681	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4039384 (Security Update)	Important	Information Disclosure	4022887	Base: 5.50 Temporal: 5.00 Vector:	Unknown

CVE-2017-8678						
Systems Service Pack 2					CVSS: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)	4039384 (Security Update)	Important	Information Disclosure	4022887	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4039384 (Security Update)	Important	Information Disclosure	4022887	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown

CVE-2017-8678						
Windows Server 2008 for x64-based Systems Service Pack 2	4039384 (Security Update)	Important	Information Disclosure	4022887	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4039384 (Security Update)	Important	Information Disclosure	4022887	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 R2 for Itanium-	4038777 (Monthly Rollup) 4038779	Important	Information Disclosure	4034664	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8678						
Based Systems Service Pack 1	(Security Only)					
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8678						
installation)						
Windows Server 2012	4038786 (Security Only) 4038799 (Monthly Rollup)	Important	Information Disclosure	4034665	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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)	4038786 (Security Only) 4038799 (Monthly Rollup)	Important	Information Disclosure	4034665	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Information Disclosure	4034681	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8678						
Windows Server 2012 R2 (Server Core installation)	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Information Disclosure	4034681	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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)	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8679 - Windows Kernel Information Disclosure Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8679 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 user'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:** None **Mitigations:** None **Workarounds:**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8679						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	4038781 (Security Update)	Important	Information Disclosure	4034668	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8679						
Windows 10 for x64-based Systems	4038781 (Security Update)	Important	Information Disclosure	4034668	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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 1511 for 32-bit Systems	4038783 (Security Update)	Important	Information Disclosure	4034660	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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 1511 for x64-based Systems	4038783 (Security Update)	Important	Information Disclosure	4034660	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 5.50 Temporal: 5.00 Vector:	Yes

CVE-2017-8679						
x64-based Systems					CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1703 for 32-bit Systems	4038788 (Security Update)	Important	Information Disclosure	4034674	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038788 (Security Update)	Important	Information Disclosure	4034674	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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 32-bit Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038777 (Monthly Rollup) 4038779	Important	Information Disclosure	4034664	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8679						
Service Pack 1	(Security Only)					
Windows 8.1 for 32-bit systems	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Information Disclosure	4034681	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Information Disclosure	4034681	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038792 (Monthly Rollup)	Important	Information Disclosure	4034681	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038874 (Security Update)	Important	Information Disclosure	4022013	Base: 5.50 Temporal: 5.00 Vector:	Unknown

CVE-2017-8679						
Systems Service Pack 2					CVSS: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)	4038874 (Security Update)	Important	Information Disclosure	4022013	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4038874 (Security Update)	Important	Information Disclosure	4022013	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown

CVE-2017-8679						
Windows Server 2008 for x64-based Systems Service Pack 2	4038874 (Security Update)	Important	Information Disclosure	4022013	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4038874 (Security Update)	Important	Information Disclosure	4022013	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 R2 for Itanium-	4038777 (Monthly Rollup) 4038779	Important	Information Disclosure	4034664	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8679						
Based Systems Service Pack 1	(Security Only)					
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8679						
installation)						
Windows Server 2012	4038786 (Security Only) 4038799 (Monthly Rollup)	Important	Information Disclosure	4034665	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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)	4038786 (Security Only) 4038799 (Monthly Rollup)	Important	Information Disclosure	4034665	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Information Disclosure	4034681	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8679						
Windows Server 2012 R2 (Server Core installation)	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Information Disclosure	4034681	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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)	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8680 - Win32k Information Disclosure Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8680 MITRE NVD	**CVE Title:** Win32k Information Disclosure Vulnerability **Description:** A information disclosure vulnerability exists when the Windows GDI+ component improperly discloses kernel memory addresses. An attacker who successfully exploited the vulnerability could obtain information to further compromise the user'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 security update addresses the vulnerability by correcting how the Windows GDI+ component handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8680						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8680						
Windows 7 for x64-based Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Information Disclosure	4034681	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Information Disclosure	4034681	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038792 (Monthly Rollup)	Important	Information Disclosure	4034681	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8680						
Windows Server 2008 for 32-bit Systems Service Pack 2	4039384 (Security Update)	Important	Information Disclosure	4022887	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4039384 (Security Update)	Important	Information Disclosure	4022887	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for Itanium-Based	4039384 (Security Update)	Important	Information Disclosure	4022887	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown

CVE-2017-8680						
Systems Service Pack 2						
Windows Server 2008 for x64-based Systems Service Pack 2	4039384 (Security Update)	Important	Information Disclosure	4022887	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4039384 (Security Update)	Important	Information Disclosure	4022887	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown

CVE-2017-8680						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8680						
Service Pack 1 (Server Core installation)						
Windows Server 2012	4038786 (Security Only) 4038799 (Monthly Rollup)	Important	Information Disclosure	4034665	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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)	4038786 (Security Only) 4038799 (Monthly Rollup)	Important	Information Disclosure	4034665	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038792 (Monthly Rollup) 4038793	Important	Information Disclosure	4034681	Base: 5.50 Temporal: 5.00 Vector:	Yes

CVE-2017-8680						
	(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 2012 R2 (Server Core installation)	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Information Disclosure	4034681	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8681 - Win32k Information Disclosure Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8681	**CVE Title:** Win32k Information Disclosure Vulnerability **Description:**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	A information disclosure vulnerability exists when the Windows GDI+ component improperly discloses kernel memory addresses. An attacker who successfully exploited the vulnerability could obtain information to further compromise the user'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 security update addresses the vulnerability by correcting how the Windows GDI+ component handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8681						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	4038781 (Security Update)	Important	Information Disclosure	4034668	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038781 (Security Update)	Important	Information Disclosure	4034668	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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 1511 for 32-bit Systems	4038783 (Security Update)	Important	Information Disclosure	4034660	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8681						
Windows 10 Version 1511 for x64-based Systems	4038783 (Security Update)	Important	Information Disclosure	4034660	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038788 (Security Update)	Important	Information Disclosure	4034674	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038788 (Security Update)	Important	Information Disclosure	4034674	Base: 5.50 Temporal: 5.00 Vector:	Yes

CVE-2017-8681						
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 7 for 32-bit Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Information Disclosure	4034681	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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-	4038792 (Monthly Rollup)	Important	Information Disclosure	4034681	Base: 5.50 Temporal: 5.00 Vector:	Yes

CVE-2017-8681						
based systems	4038793 (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 RT 8.1	4038792 (Monthly Rollup)	Important	Information Disclosure	4034681	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4039384 (Security Update)	Important	Information Disclosure	4022887	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server	4039384 (Security Update)	Important	Information Disclosure	4022887	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown

CVE-2017-8681						
Core installation)						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4039384 (Security Update)	Important	Information Disclosure	4022887	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for x64-based Systems Service Pack 2	4039384 (Security Update)	Important	Information Disclosure	4022887	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for x64-based Systems	4039384 (Security Update)	Important	Information Disclosure	4022887	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown

CVE-2017-8681						
Service Pack 2 (Server Core installation)						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8681						
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038786 (Security Only) 4038799 (Monthly Rollup)	Important	Information Disclosure	4034665	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2012 (Server Core	4038786 (Security Only) 4038799	Important	Information Disclosure	4034665	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2017-8681						
installation)	(Monthly Rollup)					
Windows Server 2012 R2	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Information Disclosure	4034681	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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)	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Information Disclosure	4034681	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 5.50 Temporal: 5.00 Vector:	Yes

CVE-2017-8681						
(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	

CVE-2017-8682 - Win32k Graphics Remote Code Execution Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8682 MITRE NVD	**CVE Title:** Win32k Graphics Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts. 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.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 this vulnerability. • In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit this vulnerability and then convince a user 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 click a link in an email message or in an Instant Messenger message that takes users to the attacker's website, or by opening an attachment sent through email. • In a file sharing attack scenario, an attacker could provide a specially crafted document file that is designed to exploit this vulnerability, and then convince a user to open the document file. The security update addresses the vulnerabilities by correcting how the Windows font library handles embedded fonts. **FAQ:** None **Mitigations:** None **Workarounds:**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8682						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Office 2007 Service Pack 3	3213641 (Security Update)	Critical	Remote Code Execution	None	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack	3213638 (Security Update)	Critical	Remote Code Execution	3191848	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-8682						
2 (32-bit editions)						
Microsoft Office 2010 Service Pack 2 (64-bit editions)	3213638 (Security Update)	Critical	Remote Code Execution	3191848	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office Word Viewer	4011134 (Security Update)	Critical	Remote Code Execution	3203484	Base: N/A Temporal: N/A Vector: N/A	Maybe
Windows 10 for 32-bit Systems	4038781 (Security Update)	Critical	Remote Code Execution	4034668	Base: 8.40 Temporal: 7.60 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 x64-based Systems	4038781 (Security Update)	Critical	Remote Code Execution	4034668	Base: 8.40 Temporal: 7.60 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 1511 for 32-bit Systems	4038783 (Security Update)	Critical	Remote Code Execution	4034660	Base: 8.40 Temporal: 7.60 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-2017-8682						
Windows 10 Version 1511 for x64-based Systems	4038783 (Security Update)	Critical	Remote Code Execution	4034660	Base: 8.40 Temporal: 7.60 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	4038782 (Security Update)	Critical	Remote Code Execution	4034658	Base: 8.40 Temporal: 7.60 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	4038782 (Security Update)	Critical	Remote Code Execution	4034658	Base: 8.40 Temporal: 7.60 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 32-bit Systems	4038788 (Security Update)	Critical	Remote Code Execution	4034674	Base: 8.40 Temporal: 7.60 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	4038788 (Security Update)	Critical	Remote Code Execution	4034674	Base: 8.40 Temporal: 7.60 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-2017-8682						
Windows 7 for 32-bit Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Critical	Remote Code Execution	4034664	Base: 8.40 Temporal: 7.60 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	4038777 (Monthly Rollup) 4038779 (Security Only)	Critical	Remote Code Execution	4034664	Base: 8.40 Temporal: 7.60 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	4038792 (Monthly Rollup) 4038793 (Security Only)	Critical	Remote Code Execution	4034681	Base: 8.40 Temporal: 7.60 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 x64-based systems	4038792 (Monthly Rollup) 4038793	Critical	Remote Code Execution	4034681	Base: 8.40 Temporal: 7.60 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-2017-8682						
	(Security Only)					
Windows RT 8.1	4038792 (Monthly Rollup)	Critical	Remote Code Execution	4034681	Base: 8.40 Temporal: 7.60 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 Systems Service Pack 2	4039384 (Security Update)	Critical	Remote Code Execution	4022887	Base: 8.40 Temporal: 7.60 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	Unknown
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4039384 (Security Update)	Critical	Remote Code Execution	4022887	Base: 8.40 Temporal: 7.60 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	Unknown
Windows Server 2008 for Itanium-	4039384 (Security Update)	Critical	Remote Code Execution	4022887	Base: 8.40 Temporal: 7.60	Unknown

CVE-2017-8682						
Based Systems Service Pack 2					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 x64-based Systems Service Pack 2	4039384 (Security Update)	Critical	Remote Code Execution	4022887	Base: 8.40 Temporal: 7.60 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	Unknown
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4039384 (Security Update)	Critical	Remote Code Execution	4022887	Base: 8.40 Temporal: 7.60 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	Unknown
Windows Server 2008 R2 for	4038777 (Monthly Rollup)	Critical	Remote Code Execution	4034664	Base: 8.40 Temporal: 7.60	Yes

CVE-2017-8682						
Itanium-Based Systems Service Pack 1	4038779 (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 R2 for x64-based Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Critical	Remote Code Execution	4034664	Base: 8.40 Temporal: 7.60 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 (Server Core installation)	4038777 (Monthly Rollup) 4038779 (Security Only)	Critical	Remote Code Execution	4034664	Base: 8.40 Temporal: 7.60 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-2017-8682						
Windows Server 2012	4038786 (Security Only) 4038799 (Monthly Rollup)	Critical	Remote Code Execution	4034665	Base: 8.40 Temporal: 7.60 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)	4038786 (Security Only) 4038799 (Monthly Rollup)	Critical	Remote Code Execution	4034665	Base: 8.40 Temporal: 7.60 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	4038792 (Monthly Rollup) 4038793 (Security Only)	Critical	Remote Code Execution	4034681	Base: 8.40 Temporal: 7.60 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)	4038792 (Monthly Rollup) 4038793	Critical	Remote Code Execution	4034681	Base: 8.40 Temporal: 7.60 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-2017-8682						
	(Security Only)					
Windows Server 2016	4038782 (Security Update)	Critical	Remote Code Execution	4034658	Base: 8.40 Temporal: 7.60 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)	4038782 (Security Update)	Critical	Remote Code Execution	4034658	Base: 8.40 Temporal: 7.60 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-2017-8683 - Win32k Graphics Information Disclosure Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8683	**CVE Title:** Win32k Graphics Information Disclosure Vulnerability **Description:**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	An information disclosure vulnerability exists when the Microsoft Windows Graphics Component improperly handles objects in memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the user'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 the way in which the Windows Graphics Component handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8683						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	4038781 (Security Update)	Important	Information Disclosure	4034668	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038781 (Security Update)	Important	Information Disclosure	4034668	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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 1511 for 32-bit Systems	4038783 (Security Update)	Important	Information Disclosure	4034660	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8683						
Windows 10 Version 1511 for x64-based Systems	4038783 (Security Update)	Important	Information Disclosure	4034660	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038788 (Security Update)	Important	Information Disclosure	4034674	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038788 (Security Update)	Important	Information Disclosure	4034674	Base: 5.50 Temporal: 5.00 Vector:	Yes

CVE-2017-8683						
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 7 for 32-bit Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Information Disclosure	4034681	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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-	4038792 (Monthly Rollup)	Important	Information Disclosure	4034681	Base: 5.50 Temporal: 5.00 Vector:	Yes

CVE-2017-8683						
based systems	4038793 (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	4039384 (Security Update)	Important	Information Disclosure	4022887	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4039384 (Security Update)	Important	Information Disclosure	4022887	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown

CVE-2017-8683						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4039384 (Security Update)	Important	Information Disclosure	4022887	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for x64-based Systems Service Pack 2	4039384 (Security Update)	Important	Information Disclosure	4022887	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for x64-based Systems Service Pack 2 (Server	4039384 (Security Update)	Important	Information Disclosure	4022887	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown

CVE-2017-8683						
Core installation)						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038777 (Monthly Rollup)	Important	Information Disclosure	4034664	Base: 5.50 Temporal: 5.00 Vector:	Yes

CVE-2017-8683						
for x64-based Systems Service Pack 1 (Server Core installation)	4038779 (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 2012	4038786 (Security Only) 4038799 (Monthly Rollup)	Important	Information Disclosure	4034665	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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)	4038786 (Security Only) 4038799 (Monthly Rollup)	Important	Information Disclosure	4034665	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8683						
Windows Server 2012 R2	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Information Disclosure	4034681	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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)	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Information Disclosure	4034681	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8683						
installation)						

CVE-2017-8684 - Windows GDI+ Information Disclosure Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8684 MITRE NVD	**CVE Title:** Windows GDI+ Information Disclosure Vulnerability **Description:** A information disclosure vulnerability exists when the Windows GDI+ component improperly discloses kernel memory addresses. An attacker who successfully exploited the vulnerability could obtain information to further compromise the user'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 security update addresses the vulnerability by correcting how the Windows GDI+ component handles objects in memory.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8684						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2017-8684						
Windows 7 for 32-bit Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Information Disclosure	4034681	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038792 (Monthly Rollup) 4038793	Important	Information Disclosure	4034681	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8684						
	(Security Only)					
Windows RT 8.1	4038792 (Monthly Rollup)	Important	Information Disclosure	4034681	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4039384 (Security Update)	Important	Information Disclosure	4022887	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core	4039384 (Security Update)	Important	Information Disclosure	4022887	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown

CVE-2017-8684						
installation)						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4039384 (Security Update)	Important	Information Disclosure	4022887	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for x64-based Systems Service Pack 2	4039384 (Security Update)	Important	Information Disclosure	4022887	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for x64-based Systems Service	4039384 (Security Update)	Important	Information Disclosure	4022887	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown

CVE-2017-8684						
Pack 2 (Server Core installation)						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8684						
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038786 (Security Only) 4038799 (Monthly Rollup)	Important	Information Disclosure	4034665	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038786 (Security Only) 4038799	Important	Information Disclosure	4034665	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8684						
installation)	(Monthly Rollup)					
Windows Server 2012 R2	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Information Disclosure	4034681	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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)	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Information Disclosure	4034681	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8685 - Windows GDI+ Information Disclosure Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8685 MITRE NVD	**CVE Title:** Windows GDI+ Information Disclosure Vulnerability **Description:** A information disclosure vulnerability exists when the Windows GDI+ component improperly discloses kernel memory addresses. An attacker who successfully exploited the vulnerability could obtain information to further compromise the user'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 security update addresses the vulnerability by correcting how the Windows GDI+ component handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information published.	Important	Information Disclosure

Affected Software

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

CVE-2017-8685						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4039384 (Security Update)	Important	Information Disclosure	4022887	Base: 5.50 Temporal: 5.00 Vector:	Unknown

CVE-2017-8685						
Systems Service Pack 2					CVSS: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)	4039384 (Security Update)	Important	Information Disclosure	4022887	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4039384 (Security Update)	Important	Information Disclosure	4022887	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown

CVE-2017-8685						
Windows Server 2008 for x64-based Systems Service Pack 2	4039384 (Security Update)	Important	Information Disclosure	4022887	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4039384 (Security Update)	Important	Information Disclosure	4022887	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 R2 for Itanium-	4038777 (Monthly Rollup) 4038779	Important	Information Disclosure	4034664	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8685						
Based Systems Service Pack 1	(Security Only)					
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8685						
installation)						

CVE-2017-8686 - Windows DHCP Server Remote Code Execution Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8686 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 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.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information published. 1.1 2017-09-12T07:00:00 Added a mitigation stating that customers who have not configured their DHCP server as a failover are not affected by this vulnerability. This is an informational change only.		

Affected Software

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

CVE-2017-8686						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows Server 2012	4038786 (Security Only) 4038799 (Monthly Rollup)	Critical	Remote Code Execution	4034665	Base: 9.80 Temporal: 8.80 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)	4038786 (Security Only) 4038799 (Monthly Rollup)	Critical	Remote Code Execution	4034665	Base: 9.80 Temporal: 8.80 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	4038792 (Monthly Rollup) 4038793 (Security Only)	Critical	Remote Code Execution	4034681	Base: 9.80 Temporal: 8.80 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 (Server	4038792 (Monthly Rollup)	Critical	Remote Code Execution	4034681	Base: 9.80 Temporal: 8.80	Yes

CVE-2017-8686						
Core installation)	4038793 (Security Only)				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	
Windows Server 2016	4038782 (Security Update)	Critical	Remote Code Execution	4034658	Base: 9.80 Temporal: 8.80 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)	4038782 (Security Update)	Critical	Remote Code Execution	4034658	Base: 9.80 Temporal: 8.80 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-2017-8687 - Win32k Information Disclosure Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8687 MITRE NVD	**CVE Title:** Win32k Information Disclosure Vulnerability **Description:** An Information disclosure vulnerability exists in Windows kernel that could allow an attacker to retrieve information that could lead to a Kernel Address Space Layout Randomization (KASLR) bypass. An attacker who successfully exploited this vulnerability could retrieve the memory address of a kernel object. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The security update addresses the vulnerability by correcting how the Windows kernel handles memory addresses. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information published.	Important	Information Disclosure

Affected Software

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

CVE-2017-8687						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	4038781 (Security Update)	Important	Information Disclosure	4034668	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038781 (Security Update)	Important	Information Disclosure	4034668	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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 1511 for 32-bit Systems	4038783 (Security Update)	Important	Information Disclosure	4034660	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8687						
Windows 10 Version 1511 for x64-based Systems	4038783 (Security Update)	Important	Information Disclosure	4034660	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038788 (Security Update)	Important	Information Disclosure	4034674	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038788 (Security Update)	Important	Information Disclosure	4034674	Base: 5.50 Temporal: 5.00 Vector:	Yes

CVE-2017-8687						
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 7 for 32-bit Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Information Disclosure	4034681	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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-	4038792 (Monthly Rollup)	Important	Information Disclosure	4034681	Base: 5.50 Temporal: 5.00 Vector:	Yes

CVE-2017-8687						
based systems	4038793 (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 RT 8.1	4038792 (Monthly Rollup)	Important	Information Disclosure	4034681	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4039384 (Security Update)	Important	Information Disclosure	4022887	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server	4039384 (Security Update)	Important	Information Disclosure	4022887	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown

CVE-2017-8687						
Core installation)						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4039384 (Security Update)	Important	Information Disclosure	4022887	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for x64-based Systems Service Pack 2	4039384 (Security Update)	Important	Information Disclosure	4022887	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for x64-based Systems	4039384 (Security Update)	Important	Information Disclosure	4022887	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown

CVE-2017-8687						
Service Pack 2 (Server Core installation)						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8687						
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038786 (Security Only) 4038799 (Monthly Rollup)	Important	Information Disclosure	4034665	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038786 (Security Only) 4038799	Important	Information Disclosure	4034665	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8687						
installation)	(Monthly Rollup)					
Windows Server 2012 R2	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Information Disclosure	4034681	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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)	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Information Disclosure	4034681	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 5.50 Temporal: 5.00 Vector:	Yes

CVE-2017-8687						
(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	

CVE-2017-8688 - Windows GDI+ Information Disclosure Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8688 MITRE NVD	**CVE Title:** Windows GDI+ Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists in the way that the Windows Graphics Device Interface+ (GDI+) handles objects in memory, allowing an attacker to retrieve information from a targeted system. By itself, the information disclosure does not allow arbitrary code execution; however, it could allow arbitrary code to be run if the attacker uses it in combination with another vulnerability. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by correcting how GDI+ handles memory addresses. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8688						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	4038781 (Security Update)	Important	Information Disclosure	4034668	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038781 (Security Update)	Important	Information Disclosure	4034668	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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 1511 for 32-bit Systems	4038783 (Security Update)	Important	Information Disclosure	4034660	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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 1511 for x64-based Systems	4038783 (Security Update)	Important	Information Disclosure	4034660	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8688						
Windows 10 Version 1607 for 32-bit Systems	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038788 (Security Update)	Important	Information Disclosure	4034674	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038788 (Security Update)	Important	Information Disclosure	4034674	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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 32-bit Systems	4038777 (Monthly Rollup)	Important	Information Disclosure	4034664	Base: 5.50 Temporal: 5.00 Vector:	Yes

CVE-2017-8688						
Service Pack 1	4038779 (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 7 for x64-based Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Information Disclosure	4034681	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Information Disclosure	4034681	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8688						
Windows RT 8.1	4038792 (Monthly Rollup)	Important	Information Disclosure	4034681	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4039384 (Security Update)	Important	Information Disclosure	4022887	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4039384 (Security Update)	Important	Information Disclosure	4022887	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown

CVE-2017-8688						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4039384 (Security Update)	Important	Information Disclosure	4022887	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for x64-based Systems Service Pack 2	4039384 (Security Update)	Important	Information Disclosure	4022887	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for x64-based Systems Service Pack 2 (Server	4039384 (Security Update)	Important	Information Disclosure	4022887	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown

CVE-2017-8688						
Core installation)						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038777 (Monthly Rollup)	Important	Information Disclosure	4034664	Base: 5.50 Temporal: 5.00 Vector:	Yes

CVE-2017-8688						
for x64-based Systems Service Pack 1 (Server Core installation)	4038779 (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 2012	4038786 (Security Only) 4038799 (Monthly Rollup)	Important	Information Disclosure	4034665	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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)	4038786 (Security Only) 4038799 (Monthly Rollup)	Important	Information Disclosure	4034665	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8688						
Windows Server 2012 R2	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Information Disclosure	4034681	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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)	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Information Disclosure	4034681	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/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	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8688						
installation)						

CVE-2017-9417 - Broadcom BCM43xx Remote Code Execution Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-9417 MITRE NVD	**CVE Title:** Broadcom BCM43xx Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when the Broadcom chipset in HoloLens improperly handles objects in memory. An attacker who successfully exploited this 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. To exploit this vulnerability, an attacker would need to send a specially crafted WiFi packet.	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The update addresses the vulnerability by correcting how the Broadcom chipset in HoloLens handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-9417						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2017-9417						
Windows 10 Version 1607 for 32-bit Systems	4038782 (Security Update)	Important	Remote Code Execution	4034658	Base: 8.80 Temporal: 8.20 Vector: CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Yes

ADV170013 - September 2017 Flash Security Update

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
ADV170013 MITRE NVD	**CVE Title:** September 2017 Flash Security Update **Description:** This security update addresses the following vulnerabilities, which are described in Adobe Security Bulletin APSB17-28: CVE-2017-11281, CVE-2017-11282. **FAQ:**	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	How could an attacker exploit these vulnerabilities? In a web-based attack scenario where the user is using Internet Explorer for the desktop, an attacker could host a specially crafted website that is designed to exploit any of these vulnerabilities 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 any of these vulnerabilities. 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 by clicking a link in an email message or in an Instant Messenger message that takes users to the attacker's website, or by opening an attachment sent through email. In a web-based attack scenario where the user is using Internet Explorer in the Windows 8-style UI, an attacker would first need to compromise a website already listed in the Compatibility View (CV) list. An attacker could then host a website that contains specially crafted Flash content designed to exploit any of these vulnerabilities through Internet Explorer and then convince a user 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 clicking a link in an email message or in an Instant Messenger		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	message that takes users to the attacker's website, or by opening an attachment sent through email. For more information about Internet Explorer and the CV List, please see the MSDN Article, Developer Guidance for websites with content for Adobe Flash Player in Windows 8. **Mitigations:** **Workarounds:** Workaround refers to a setting or configuration change that would help block known attack vectors before you apply the update. • **Prevent Adobe Flash Player from running** You can disable attempts to instantiate Adobe Flash Player in Internet Explorer and other applications that honor the kill bit feature, such as Office 2007 and Office 2010, by setting the kill bit for the control in the registry. **Warning** If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that you can solve problems that result from using Registry Editor incorrectly. Use Registry Editor at your own risk. To set the kill bit for the control in the registry, perform the following steps: 1. Paste the following into a text file and save it with the .reg file extension. Copy		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Windows Registry Editor Version 5.00 [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX Compatibility\{D27CDB6E-AE6D-11CF-96B8-444553540000}] "Compatibility Flags"=dword:00000400 [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\ActiveX Compatibility\{D27CDB6E-AE6D-11CF-96B8-444553540000}] "Compatibility Flags"=dword:00000400 2. Double-click the .reg file to apply it to an individual system. You can also apply this workaround across domains by using Group Policy. For more information about Group Policy, see the TechNet article, Group Policy collection. **Note** You must restart Internet Explorer for your changes to take effect. **Impact of workaround**. There is no impact as long as the object is not intended to be used in Internet Explorer. **How to undo the workaround.** Delete the registry keys that were added in implementing this workaround.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	• **Prevent Adobe Flash Player from running in Internet Explorer through Group Policy** **Note** The Group Policy MMC snap-in can be used to set policy for a machine, for an organizational unit, or for an entire domain. For more information about Group Policy, visit the following Microsoft Web sites: Group Policy Overview What is Group Policy Object Editor? Core Group Policy tools and settings To disable Adobe Flash Player in Internet Explorer through Group Policy, perform the following steps: **Note** This workaround does not prevent Flash from being invoked from other applications, such as Microsoft Office 2007 or Microsoft Office 2010. 1. Open the Group Policy Management Console and configure the console to work with the appropriate Group Policy object, such as local machine, OU, or domain GPO. 2. Navigate to the following node: **Administrative Templates** -> **Windows Components** -> **Internet Explorer** -> **Security Features** -> **Add-on Management**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	3. Double-click **Turn off Adobe Flash in Internet Explorer and prevent applications from using Internet Explorer technology to instantiate Flash objects**. 4. Change the setting to **Enabled**. 5. Click **Apply** and then click **OK** to return to the Group Policy Management Console. 6. Refresh Group Policy on all systems or wait for the next scheduled Group Policy refresh interval for the settings to take effect. • **Prevent Adobe Flash Player from running in Office 2010 on affected systems** **Note** This workaround does not prevent Adobe Flash Player from running in Internet Explorer. **Warning** If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that you can solve problems that result from using Registry Editor incorrectly. Use Registry Editor at your own risk. For detailed steps that you can use to prevent a control from running in Internet Explorer, see Microsoft Knowledge Base Article 240797. Follow the steps in the article to create a Compatibility Flags value in the registry to prevent a COM object from being instantiated in Internet Explorer.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	To disable Adobe Flash Player in Office 2010 only, set the kill bit for the ActiveX control for Adobe Flash Player in the registry using the following steps: 1. Create a text file named Disable_Flash.reg with the following contents: Copy Windows Registry Editor Version 5.00 [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\Common\COM\Compatibility\{D27CDB6E-AE6D-11CF-96B8-444553540000}] "Compatibility Flags"=dword:00000400 2. Double-click the .reg file to apply it to an individual system. 3. **Note** You must restart Internet Explorer for your changes to take effect. You can also apply this workaround across domains by using Group Policy. For more information about Group Policy, see the TechNet article, Group Policy collection. • **Prevent ActiveX controls from running in Office 2007 and Office 2010** To disable all ActiveX controls in Microsoft Office 2007 and Microsoft Office 2010, including Adobe Flash Player in Internet Explorer, perform the following steps: 1. Click **File**, click **Options**, click **Trust Center**, and then click **Trust Center Settings**.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	2. Click **ActiveX Settings** in the left-hand pane, and then select **Disable all controls without notifications**. 3. Click **OK** to save your settings. **Impact of workaround.** Office documents that use embedded ActiveX controls may not display as intended. **How to undo the workaround.** To re-enable ActiveX controls in Microsoft Office 2007 and Microsoft Office 2010, perform the following steps: 4. Click **File**, click **Options**, click **Trust Center**, and then click **Trust Center Settings**. 5. Click **ActiveX Settings** in the left-hand pane, and then deselect **Disable all controls without notifications**. 6. Click **OK** to save your settings. • **Set Internet and Local intranet security zone settings to "High" to block ActiveX Controls and Active Scripting in these zones** You can help protect against exploitation of these vulnerabilities by changing your settings for the Internet security zone to block ActiveX controls and Active Scripting. You can do this by setting your browser security to High. To raise the browsing security level in Internet Explorer, perform the following steps:		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	1. On the Internet Explorer **Tools** menu, click **Internet Options**. 2. In the **Internet Options** dialog box, click the **Security** tab, and then click **Internet**. 3. Under **Security level for this zone**, move the slider to **High**. This sets the security level for all websites you visit to High. 4. Click **Local intranet**. 5. Under **Security level for this zone**, move the slider to **High**. This sets the security level for all websites you visit to High. 6. Click **OK** to accept the changes and return to Internet Explorer. **Note** If no slider is visible, click **Default Level**, and then move the slider to **High**. **Note** Setting the level to High may cause some websites to work incorrectly. If you have difficulty using a website after you change this setting, and you are sure the site is safe to use, you can add that site to your list of trusted sites. This will allow the site to work correctly even with the security setting set to High. **Impact of workaround.** There are side effects to blocking ActiveX Controls and Active Scripting. Many websites on the Internet or an intranet use ActiveX or Active Scripting to provide additional functionality. For example, an online e-commerce site or banking site may use ActiveX Controls to provide menus, ordering forms, or even account statements. Blocking ActiveX Controls or Active Scripting is a global setting that affects all Internet and intranet		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	sites. If you do not want to block ActiveX Controls or Active Scripting for such sites, use the steps outlined in "Add sites that you trust to the Internet Explorer Trusted sites zone". • **Configure Internet Explorer to prompt before running Active Scripting or to disable Active Scripting in the Internet and Local intranet security zone** You can help protect against exploitation of these vulnerabilities by changing your settings to prompt before running Active Scripting or to disable Active Scripting in the Internet and Local intranet security zone. To do this, perform the following steps: 1. In Internet Explorer, click **Internet Options** on the **Tools** menu. 2. Click the **Security** tab. 3. Click **Internet**, and then click **Custom Level**. 4. Under **Settings**, in the **Scripting** section, under **Active Scripting**, click **Prompt** or **Disable**, and then click **OK**. 5. Click **Local intranet**, and then click **Custom Level**. 6. Under **Settings**, in the **Scripting** section, under **Active Scripting**, click **Prompt** or **Disable**, and then click **OK**. 7. Click **OK** to return to Internet Explorer, and then click **OK** again. **Note** Disabling Active Scripting in the Internet and Local intranet security zones may cause some websites to work incorrectly. If you have difficulty using a website after you change this		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	setting, and you are sure the site is safe to use, you can add that site to your list of trusted sites. This will allow the site to work correctly. **Impact of workaround.** There are side effects to prompting before running Active Scripting. Many websites that are on the Internet or on an intranet use Active Scripting to provide additional functionality. For example, an online e-commerce site or banking site may use Active Scripting to provide menus, ordering forms, or even account statements. Prompting before running Active Scripting is a global setting that affects all Internet and intranet sites. You will be prompted frequently when you enable this workaround. For each prompt, if you feel you trust the site that you are visiting, click **Yes** to run Active Scripting. If you do not want to be prompted for all these sites, use the steps outlined in "Add sites that you trust to the Internet Explorer Trusted sites zone". • **Add sites that you trust to the Internet Explorer Trusted sites zone** After you set Internet Explorer to require a prompt before it runs ActiveX controls and Active Scripting in the Internet zone and in the Local intranet zone, you can add sites that you trust to the Internet Explorer Trusted sites zone. This will allow you to continue to use trusted websites exactly as you do today, while helping to protect you from this attack on untrusted sites. We recommend that you add only sites that you trust to the Trusted sites zone. To do this, perform the following steps:		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	1. In Internet Explorer, click **Tools**, click **Internet Options**, and then click the **Security** tab. 2. In the **Select a web content zone to specify its current security settings** box, click **Trusted Sites**, and then click **Sites**. 3. If you want to add sites that do not require an encrypted channel, click to clear the **Require server verification (https:) for all sites in this zone** check box. 4. In the **Add this website to the zone** box, type the URL of a site that you trust, and then click **Add**. 5. Repeat these steps for each site that you want to add to the zone. 6. Click **OK** two times to accept the changes and return to Internet Explorer. **Note** Add any sites that you trust not to take malicious action on your system. Two sites in particular that you may want to add are ***.windowsupdate.microsoft.com** and ***.update.microsoft.com**. These are the sites that will host the update, and they require an ActiveX control to install the update. **Revision:** 1.0 2017-09-12T07:00:00 Information Published.		

Affected Software

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

ADV170013						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Adobe Flash Player on Windows 10 for 32-bit Systems	4038806 (Security Update)	Critical	Remote Code Execution	4034662	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 for x64-based Systems	4038806 (Security Update)	Critical	Remote Code Execution	4034662	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1511 for 32-bit Systems	4038806 (Security Update)	Critical	Remote Code Execution	4034662	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1511 for x64-based Systems	4038806 (Security Update)	Critical	Remote Code Execution	4034662	Base: N/A Temporal: N/A Vector: N/A	Yes

ADV170013						
Adobe Flash Player on Windows 10 Version 1607 for 32-bit Systems	4038806 (Security Update)	Critical	Remote Code Execution	4034662	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1607 for x64-based Systems	4038806 (Security Update)	Critical	Remote Code Execution	4034662	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1703 for 32-bit Systems	4038806 (Security Update)	Critical	Remote Code Execution	4034662	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1703 for x64-based Systems	4038806 (Security Update)	Critical	Remote Code Execution	4034662	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 8.1 for 32-bit systems	4038806 (Security Update)	Critical	Remote Code Execution	4034662	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 8.1 for x64-based systems	4038806 (Security Update)	Critical	Remote Code Execution	4034662	Base: N/A Temporal:	Yes

ADV170013						
					N/A Vector: N/A	
Adobe Flash Player on Windows RT 8.1	4038806 (Security Update)	Critical	Remote Code Execution	4034662	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows Server 2012	4038806 (Security Update)	Critical	Remote Code Execution	4034662	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows Server 2012 R2	4038806 (Security Update)	Critical	Remote Code Execution	4034662	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows Server 2016	4038806 (Security Update)	Critical	Remote Code Execution	4034662	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2017-8744 - Microsoft Office Memory Corruption Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8744 MITRE NVD	**CVE Title:** Microsoft Office Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in Microsoft Office software when it fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could use a specially crafted file to perform actions in the security context of the current user. For example, the file could then take actions on behalf of the logged-on user with the same permissions as the current user. Exploitation of this vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Office software. 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) that contains a specially crafted file that is designed to exploit the vulnerability. However, an attacker would have no way to force the user to visit the website. Instead, an attacker would have to convince the user to click a link, typically by way of an enticement in an email or Instant Messenger message, and then convince the user to open the specially crafted file.	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by correcting how Microsoft Office handles files in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information Published.		

Affected Software

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

CVE-2017-8744						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2017-8744						
Microsoft Office 2007 Service Pack 3	3213646 (Security Update)	Important	Remote Code Execution	None	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (32-bit editions)	3213626 (Security Update)	Important	Remote Code Execution	3203461	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (64-bit editions)	3213626 (Security Update)	Important	Remote Code Execution	3203461	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2013 RT Service Pack 1	3213564 (Security Update)	Important	Remote Code Execution	3203392	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2013 Service Pack 1 (32-bit editions)	3213564 (Security Update)	Important	Remote Code Execution	None	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2013 Service Pack 1 (64-bit editions)	3213564 (Security Update)	Important	Remote Code Execution	None	Base: N/A Temporal:	Maybe

CVE-2017-8744						
					N/A Vector: N/A	
Microsoft Office 2016 (32-bit edition)	3213551 (Security Update)	Important	Remote Code Execution	3203383	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 (64-bit edition)	3213551 (Security Update)	Important	Remote Code Execution	3203383	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-8745 - Microsoft SharePoint Cross Site Scripting Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8745	**CVE Title:** Microsoft SharePoint Cross Site Scripting Vulnerability **Description:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	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 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:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information Published.		

Affected Software

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

CVE-2017-8745						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SharePoint Foundation 2013 Service Pack 1	4011117 (Security Update)	Important	Elevation of Privilege	None	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-8737 - Microsoft PDF Remote Code Execution Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8737 MITRE NVD	**CVE Title:** Microsoft PDF Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when Microsoft Windows PDF Library improperly handles objects in memory. The vulnerability could corrupt memory in a way that enables an attacker to execute arbitrary code in the context of the current user. 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 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. To exploit the vulnerability on Windows 10 systems with Microsoft Edge set as the default browser, an attacker could host a specially crafted website that contains malicious PDF content and then convince users 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 PDF content to such sites. Only Windows 10 systems with Microsoft Edge set as the default browser can be compromised simply by viewing a website. The browsers for all other affected operating systems do not automatically render PDF content, so an attacker would have no way to force users to view attacker-controlled content. Instead, an attacker would have to convince users to open a specially crafted PDF document, typically by way of an enticement in an email or instant message or by way of an email attachment.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The update addresses the vulnerability by modifying how affected systems handle objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8737						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2017-8737						
Microsoft Edge on Windows 10 for 32-bit Systems	4038781 (Security Update)	Critical	Remote Code Execution	4034668	Base: 4.20 Temporal: 3.80 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	4038781 (Security Update)	Critical	Remote Code Execution	4034668	Base: 4.20 Temporal: 3.80 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 1511 for 32-bit Systems	4038783 (Security Update)	Critical	Remote Code Execution	4034660	Base: 4.20 Temporal: 3.80 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 1511 for	4038783 (Security Update)	Critical	Remote Code Execution	4034660	Base: 4.20 Temporal: 3.80 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-2017-8737						
x64-based Systems						
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4038782 (Security Update)	Critical	Remote Code Execution	4034658	Base: 4.20 Temporal: 3.80 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	4038782 (Security Update)	Critical	Remote Code Execution	4034658	Base: 4.20 Temporal: 3.80 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	4038788 (Security Update)	Critical	Remote Code Execution	4034674	Base: 4.20 Temporal: 3.80 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-2017-8737						
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4038788 (Security Update)	Critical	Remote Code Execution	4034674	Base: 4.20 Temporal: 3.80 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	4038782 (Security Update)	Moderate	Remote Code Execution	4034658	Base: 3.10 Temporal: 2.80 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4038792 (Monthly Rollup) 4038793 (Security Only)	Critical	Remote Code Execution	4034681	Base: 2.60 Temporal: 2.40 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4038792 (Monthly Rollup) 4038793	Critical	Remote Code Execution	4034681	Base: 2.60 Temporal: 2.40 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8737						
	(Security Only)					
Windows RT 8.1	4038792 (Monthly Rollup)	Critical	Remote Code Execution	4034681	Base: 2.60 Temporal: 2.40 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012	4038786 (Security Only) 4038799 (Monthly Rollup)	Moderate	Remote Code Execution	4034665	Base: 2.60 Temporal: 2.40 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4038786 (Security Only) 4038799 (Monthly Rollup)	Moderate	Remote Code Execution	4034665	Base: 2.60 Temporal: 2.40 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4038792 (Monthly Rollup) 4038793	Moderate	Remote Code Execution	4034681	Base: 2.60 Temporal: 2.40 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8737						
	(Security Only)					
Windows Server 2012 R2 (Server Core installation)	4038792 (Monthly Rollup) 4038793 (Security Only)	Moderate	Remote Code Execution	4034681	Base: 2.60 Temporal: 2.40 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8748 - Scripting Engine Memory Corruption Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8748 MITRE NVD	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that Microsoft browser JavaScript engines render content when handling objects in memory. The vulnerability	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. In a web-based attack scenario, 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. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the related 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. 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. The security update addresses the vulnerability by modifying how Microsoft browser JavaScript scripting engines handle objects in memory. **FAQ:** None **Mitigations:** None		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Workarounds: None **Revision:** 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8748						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 11 on Windows 10 for 32-bit Systems	4038781 (Security Update)	Critical	Remote Code Execution	4034668	Base: 4.20 Temporal: 3.80 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-2017-8748						
Internet Explorer 11 on Windows 10 for x64-based Systems	4038781 (Security Update)	Critical	Remote Code Execution	4034668	Base: 4.20 Temporal: 3.80 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
Internet Explorer 11 on Windows 10 Version 1511 for 32-bit Systems	4038783 (Security Update)	Critical	Remote Code Execution	4034660	Base: 4.20 Temporal: 3.80 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
Internet Explorer 11 on Windows 10 Version	4038783 (Security Update)	Critical	Remote Code Execution	4034660	Base: 4.20 Temporal: 3.80 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-2017-8748						
1511 for x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems	4038782 (Security Update)	Critical	Remote Code Execution	4034658	Base: 4.20 Temporal: 3.80 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
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4038782 (Security Update)	Critical	Remote Code Execution	4034658	Base: 4.20 Temporal: 3.80 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-2017-8748						
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems	4038788 (Security Update)	Critical	Remote Code Execution	4034674	Base: 4.20 Temporal: 3.80 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
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems	4038788 (Security Update)	Critical	Remote Code Execution	4034674	Base: 4.20 Temporal: 3.80 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
Internet Explorer 11 on Windows	4038777 (Monthly Rollup)	Critical	Remote Code Execution	4034664 4034733	Base: 4.20 Temporal: 3.80 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-2017-8748						
7 for 32-bit Systems Service Pack 1	4036586 (IE Cumulative)					
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1	4038777 (Monthly Rollup) 4036586 (IE Cumulative)	Critical	Remote Code Execution	4034664 4034733	Base: 4.20 Temporal: 3.80 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
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4038792 (Monthly Rollup) 4036586 (IE Cumulative)	Critical	Remote Code Execution	4034681 4034733	Base: 4.20 Temporal: 3.80 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-2017-8748						
Internet Explorer 11 on Windows 8.1 for x64-based systems	4038792 (Monthly Rollup) 4036586 (IE Cumulative)	Critical	Remote Code Execution	4034681 4034733	Base: 4.20 Temporal: 3.80 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
Internet Explorer 11 on Windows RT 8.1	4038792 (Monthly Rollup)	Critical	Remote Code Execution	4034681	Base: 4.20 Temporal: 3.80 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
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems	4038777 (Monthly Rollup) 4036586 (IE Cumulative)	Moderate	Remote Code Execution	4034664 4034733	Base: 3.10 Temporal: 2.80 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8748						
Service Pack 1						
Internet Explorer 11 on Windows Server 2012 R2	4038792 (Monthly Rollup) 4036586 (IE Cumulative)	Moderate	Remote Code Execution	4034681 4034733	Base: 3.10 Temporal: 2.80 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2016	4038782 (Security Update)	Moderate	Remote Code Execution	4034658	Base: 3.10 Temporal: 2.80 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 for 32-bit Systems	4038781 (Security Update)	Critical	Remote Code Execution	4034668	Base: 4.20 Temporal: 3.80 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	4038781 (Security Update)	Critical	Remote Code Execution	4034668	Base: 4.20 Temporal: 3.80	Yes

CVE-2017-8748						
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 10 Version 1511 for 32-bit Systems	4038783 (Security Update)	Critical	Remote Code Execution	4034660	Base: 4.20 Temporal: 3.80 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 1511 for x64-based Systems	4038783 (Security Update)	Critical	Remote Code Execution	4034660	Base: 4.20 Temporal: 3.80 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-2017-8748						
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4038782 (Security Update)	Critical	Remote Code Execution	4034658	Base: 4.20 Temporal: 3.80 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	4038782 (Security Update)	Critical	Remote Code Execution	4034658	Base: 4.20 Temporal: 3.80 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	4038788 (Security Update)	Critical	Remote Code Execution	4034674	Base: 4.20 Temporal: 3.80 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-2017-8748						
32-bit Systems						
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4038788 (Security Update)	Critical	Remote Code Execution	4034674	Base: 4.20 Temporal: 3.80 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	4038782 (Security Update)	Moderate	Remote Code Execution	4034658	Base: 4.20 Temporal: 3.80 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-2017-8758 - Microsoft Exchange Cross-Site Scripting Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8758 MITRE NVD	**CVE Title:** Microsoft Exchange Cross-Site Scripting Vulnerability **Description:** An elevation of privilege vulnerability exists when Microsoft Exchange Outlook Web Access (OWA) fails to properly handle web requests. An attacker who successfully exploited this vulnerability could perform script/content injection attacks and attempt to trick the user into disclosing sensitive information. To exploit the vulnerability, an attacker could send a specially crafted email message containing a malicious link to a user. Alternatively, an attacker could use a chat client to social engineer a user into clicking the malicious link. The security update addresses the vulnerability by correcting how Microsoft Exchange validates web requests. Note: In order to exploit this vulnerability, a user must click a maliciously crafted link from an attacker. **FAQ:** None **Mitigations:** None **Workarounds:** None	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8758						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Exchange Server 2016 Cumulative Update 6	4036108 (Security Update)	Important	Elevation of Privilege	None	Base: N/A Temporal: N/A Vector: N/A	Yes

ADV170015 - Microsoft Office Defense in Depth Update

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
ADV170015 MITRE NVD	**CVE Title:** Microsoft Office Defense in Depth Update **Description:** Microsoft has released an update for Microsoft Office that provides enhanced security as a defense-in-depth measure. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information published.	Unkwown	Defense in Depth

Affected Software

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

ADV170015						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Office 2007 Service Pack 3	4011063 (Security Update)	None	Defense in Depth	None	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (32-bit editions)	4011055 (Security Update)	None	Defense in Depth	3213624	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (64-bit editions)	4011055 (Security Update)	None	Defense in Depth	3213624	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2013 RT Service Pack 1	4011103 (Security Update)	None	Defense in Depth	3213555	Base: N/A Temporal: N/A Vector: N/A	Maybe

ADV170015						
Microsoft Office 2013 Service Pack 1 (32-bit editions)	4011103 (Security Update)	None	Defense in Depth	3213555	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2013 Service Pack 1 (64-bit editions)	4011103 (Security Update)	None	Defense in Depth	3213555	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 (32-bit edition)	4011126 (Security Update) 4011038 (Security Update)	None	Defense in Depth	3213545 3191943	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 (64-bit edition)	4011126 (Security Update) 4011038 (Security Update)	None	Defense in Depth	3213545 3191943	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Outlook 2007 Service Pack 3	4011086 (Security Update)	None	Defense in Depth	3213643	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Outlook 2010 Service Pack 2 (32-bit editions)	4011089 (Security Update)	None	Defense in Depth	2956078	Base: N/A Temporal:	Maybe

ADV170015						
					N/A Vector: N/A	
Microsoft Outlook 2010 Service Pack 2 (64-bit editions)	4011089 (Security Update)	None	Defense in Depth	2956078	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Outlook 2013 (32-bit editions)	4011090 (Security Update)	None	Defense in Depth	4011078	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Outlook 2013 (64-bit editions)	4011090 (Security Update)	None	Defense in Depth	4011078	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Outlook 2013 RT Service Pack 1	4011090 (Security Update)	None	Defense in Depth	4011078	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Outlook 2016 (32-bit edition)	4011091 (Security Update)	None	Defense in Depth	4011052	Base: N/A Temporal: N/A Vector: N/A	Maybe

ADV170015						
Microsoft Outlook 2016 (64-bit edition)	4011091 (Security Update)	None	Defense in Depth	4011052	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-0161 - NetBIOS Remote Code Execution Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-0161 MITRE NVD	**CVE Title:** NetBIOS Remote Code Execution Vulnerability **Description:** A race condition that could lead to a remote code execution vulnerability exists in NetBT Session Services when NetBT fails to maintain certain sequencing requirements. To exploit the vulnerability, an attacker needs to be able to send specially crafted NetBT Session Service packets to an impacted system. An attacker who successfully exploits the vulnerability could execute arbitrary code on the target.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by correcting how NetBT sequences certain operations. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-0161						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2017-0161						
Windows 10 for 32-bit Systems	4038781 (Security Update)	Critical	Remote Code Execution	4034668	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4038781 (Security Update)	Critical	Remote Code Execution	4034668	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4038783 (Security Update)	Critical	Remote Code Execution	4034660	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	4038783 (Security Update)	Critical	Remote Code Execution	4034660	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/AC:H/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	4038782 (Security Update)	Critical	Remote Code Execution	4034658	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-0161						
Windows 10 Version 1607 for x64-based Systems	4038782 (Security Update)	Critical	Remote Code Execution	4034658	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/AC:H/PR:N/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	4038788 (Security Update)	Critical	Remote Code Execution	4034674	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/AC:H/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	4038788 (Security Update)	Critical	Remote Code Execution	4034674	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for 32-bit Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Critical	Remote Code Execution	4034664	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-0161						
Windows 7 for x64-based Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Critical	Remote Code Execution	4034664	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/AC:H/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	4038792 (Monthly Rollup) 4038793 (Security Only)	Critical	Remote Code Execution	4034681	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4038792 (Monthly Rollup) 4038793 (Security Only)	Critical	Remote Code Execution	4034681	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4038792 (Monthly Rollup)	Critical	Remote Code Execution	4034681	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-0161						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Critical	Remote Code Execution	4034664	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/AC:H/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	4038777 (Monthly Rollup) 4038779 (Security Only)	Critical	Remote Code Execution	4034664	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/AC:H/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 (Server	4038777 (Monthly Rollup) 4038779 (Security Only)	Critical	Remote Code Execution	4034664	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-0161						
Core installation)						
Windows Server 2012	4038786 (Security Only) 4038799 (Monthly Rollup)	Critical	Remote Code Execution	4034665	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2012 (Server Core installation)	4038786 (Security Only) 4038799 (Monthly Rollup)	Critical	Remote Code Execution	4034665	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2012 R2	4038792 (Monthly Rollup) 4038793 (Security Only)	Critical	Remote Code Execution	4034681	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4038792 (Monthly Rollup)	Critical	Remote Code Execution	4034681	Base: 8.10 Temporal: 7.30	Yes

CVE-2017-0161						
(Server Core installation)	4038793 (Security Only)				Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2016	4038782 (Security Update)	Critical	Remote Code Execution	4034658	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/AC:H/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)	4038782 (Security Update)	Critical	Remote Code Execution	4034658	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8567 - Microsoft Office Remote Code Execution

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8567 MITRE NVD	**CVE Title:** Microsoft Office Remote Code Execution **Description:** A remote code execution vulnerability exists in Microsoft Office software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Office software. 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) that contains 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. Note that the Preview Pane is not an attack vector for this vulnerability. The security update addresses the vulnerability by correcting how Office 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 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8567						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2017-8567						
Microsoft Excel for Mac 2011	3212225 (Security Update)	Important	Remote Code Execution	None	Base: N/A Temporal: N/A Vector: N/A	No

CVE-2017-8628 - Microsoft Bluetooth Driver Spoofing Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8628 MITRE NVD	**CVE Title:** Microsoft Bluetooth Driver Spoofing Vulnerability **Description:** A spoofing vulnerability exists in Microsoft's implementation of the Bluetooth stack. An attacker who successfully exploited this vulnerability could perform a man-in-the-middle attack and force a user's computer to unknowingly route traffic through the attacker's computer. The attacker can then monitor and read the traffic before sending it on to the intended recipient. To exploit the vulnerability, the attacker needs to be within the physical proximity of the targeted user, and the user's computer needs to have Bluetooth enabled. The attacker	Important	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	can then initiate a Bluetooth connection to the target computer without the user's knowledge. The security update addresses the vulnerability by correcting how Windows handles Bluetooth requests. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8628						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	4038781 (Security Update)	Important	Spoofing	4034668	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4038781 (Security Update)	Important	Spoofing	4034668	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4038783 (Security Update)	Important	Spoofing	4034660	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	4038783 (Security Update)	Important	Spoofing	4034660	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for	4038782 (Security Update)	Important	Spoofing	4034658	Base: 8.10 Temporal: 7.30	Yes

CVE-2017-8628						
32-bit Systems					Vector: CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1607 for x64-based Systems	4038782 (Security Update)	Important	Spoofing	4034658	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4038788 (Security Update)	Important	Spoofing	4034674	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4038788 (Security Update)	Important	Spoofing	4034674	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 7 for 32-bit Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Spoofing	4034664	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8628						
Windows 7 for x64-based Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Spoofing	4034664	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Spoofing	4034681	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Spoofing	4034681	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4038792 (Monthly Rollup)	Important	Spoofing	4034681	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8628						
Windows Server 2008 for 32-bit Systems Service Pack 2	4034786 (Security Update)	Important	Spoofing	4019276	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4034786 (Security Update)	Important	Spoofing	4019276	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems	4034786 (Security Update)	Important	Spoofing	None	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8628						
Service Pack 2						
Windows Server 2008 for x64-based Systems Service Pack 2	4034786 (Security Update)	Important	Spoofing	4019276	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4034786 (Security Update)	Important	Spoofing	4019276	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4038782 (Security Update)	Important	Spoofing	4034658	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8628						
Windows Server 2016 (Server Core installation)	4038782 (Security Update)	Important	Spoofing	4034658	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8643 - Microsoft Edge Information Disclosure Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8643 MITRE NVD	**CVE Title:** Microsoft Edge Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when Microsoft Edge improperly handles clipboard events. For an attack to be successful, an attacker must persuade a user to visit a malicious website and leave it open during clipboard activities. The update addresses the vulnerability by changing how Microsoft Edge handles clipboard events in the browser.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8643						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows	4038781 (Security Update)	Important	Information Disclosure	4034668	Base: 4.30 Temporal: 3.90	Yes

CVE-2017-8643						
10 for 32-bit Systems					Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 for x64-based Systems	4038781 (Security Update)	Important	Information Disclosure	4034668	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems	4038783 (Security Update)	Important	Information Disclosure	4034660	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version	4038783 (Security Update)	Important	Information Disclosure	4034660	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8643						
1511 for x64-based Systems						
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8643						
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4038788 (Security Update)	Important	Information Disclosure	4034674	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4038788 (Security Update)	Important	Information Disclosure	4034674	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server 2016	4038782 (Security Update)	Low	Information Disclosure	4034658	Base: 2.40 Temporal: 2.20 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8648 - Microsoft Edge Information Disclosure Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8648 MITRE NVD	**CVE Title:** Microsoft Edge Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when Microsoft Edge improperly handles objects in memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the user's system. To exploit the vulnerability, in a web-based attack scenario, an attacker could host a website in an attempt to exploit the vulnerability. In addition, compromised websites and websites that accept or host user-provided content could contain specially crafted content that could exploit the vulnerability. However, in all cases an attacker would have no way to force a user to view the attacker-controlled content. Instead, an attacker would have to convince a user to take action. For example, an attacker could trick a user into clicking a link that takes the user to the attacker's site. The update addresses the vulnerability by modifying how Microsoft Edge handle objects in memory. **FAQ:** None	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8648						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version	4038788 (Security Update)	Important	Information Disclosure	4034674	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8648						
1703 for 32-bit Systems						
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4038788 (Security Update)	Important	Information Disclosure	4034674	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8649 - Scripting Engine Memory Corruption Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8649 MITRE NVD	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that Microsoft browser JavaScript engines render content when handling 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. In a web-based attack scenario, 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. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the related 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. 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. The security update addresses the vulnerability by modifying how Microsoft browser JavaScript scripting engines handle objects in memory.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8649						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2017-8649						
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4038782 (Security Update)	Critical	Remote Code Execution	4034658	Base: 4.20 Temporal: 3.80 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	4038782 (Security Update)	Critical	Remote Code Execution	4034658	Base: 4.20 Temporal: 3.80 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	4038788 (Security Update)	Critical	Remote Code Execution	4034674	Base: 4.20 Temporal: 3.80 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-2017-8649						
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4038788 (Security Update)	Critical	Remote Code Execution	4034674	Base: 4.20 Temporal: 3.80 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	4038782 (Security Update)	Moderate	Remote Code Execution	4034658	Base: 3.10 Temporal: 2.80 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8660 - Scripting Engine Memory Corruption Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8660 MITRE NVD	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that Microsoft browser JavaScript engines render content when handling 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. In a web-based attack scenario, 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. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the related 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. 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. The security update addresses the vulnerability by modifying how Microsoft browser JavaScript scripting engines handle objects in memory.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8660						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2017-8660						
Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems	4038783 (Security Update)	Critical	Remote Code Execution	4034660	Base: 4.20 Temporal: 3.80 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 1511 for x64-based Systems	4038783 (Security Update)	Critical	Remote Code Execution	4034660	Base: 4.20 Temporal: 3.80 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	4038782 (Security Update)	Critical	Remote Code Execution	4034658	Base: 4.20 Temporal: 3.80 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-2017-8660						
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4038782 (Security Update)	Critical	Remote Code Execution	4034658	Base: 4.20 Temporal: 3.80 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	4038788 (Security Update)	Critical	Remote Code Execution	4034674	Base: 4.20 Temporal: 3.80 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	4038788 (Security Update)	Critical	Remote Code Execution	4034674	Base: 4.20 Temporal: 3.80 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-2017-8660						
Microsoft Edge on Windows Server 2016	4038782 (Security Update)	Moderate	Remote Code Execution	4034658	Base: 3.10 Temporal: 2.80 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8692 - Uniscribe Remote Code Execution Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8692 MITRE NVD	**CVE Title:** Uniscribe Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists due to the way Windows Uniscribe 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. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	There are multiple ways an attacker could exploit this vulnerability: • In a web-based attack scenario, an attacker could host a specially crafted website designed to exploit this vulnerability and then convince a user 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 click a link in an email or instant message that takes users to the attacker's website, or by opening an attachment sent through email. • In a file-sharing attack scenario, an attacker could provide a specially crafted document file designed to exploit this vulnerability and then convince a user to open the document file.The security update addresses the vulnerability by correcting how Windows Uniscribe handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8692						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	4038781 (Security Update)	Important	Remote Code Execution	4034668	Base: 5.00 Temporal: 4.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4038781 (Security Update)	Important	Remote Code Execution	4034668	Base: 5.00 Temporal: 4.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4038783 (Security Update)	Important	Remote Code Execution	4034660	Base: 5.00 Temporal: 4.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2017-8692						
Windows 10 Version 1511 for x64-based Systems	4038783 (Security Update)	Important	Remote Code Execution	4034660	Base: 5.00 Temporal: 4.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4038782 (Security Update)	Important	Remote Code Execution	4034658	Base: 5.00 Temporal: 4.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4038782 (Security Update)	Important	Remote Code Execution	4034658	Base: 5.00 Temporal: 4.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4038788 (Security Update)	Important	Remote Code Execution	4034674	Base: 5.00 Temporal: 4.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for	4038788 (Security Update)	Important	Remote Code Execution	4034674	Base: 5.00 Temporal: 4.50	Yes

CVE-2017-8692						
x64-based Systems					Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	
Windows 8.1 for 32-bit systems	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Remote Code Execution	4034681	Base: 5.00 Temporal: 4.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Remote Code Execution	4034681	Base: 5.00 Temporal: 4.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4038792 (Monthly Rollup)	Important	Remote Code Execution	4034681	Base: 5.00 Temporal: 4.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2012	4038786 (Security Only) 4038799	Important	Remote Code Execution	4034665	Base: 5.00 Temporal: 4.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2017-8692						
	(Monthly Rollup)					
Windows Server 2012 (Server Core installation)	4038786 (Security Only) 4038799 (Monthly Rollup)	Important	Remote Code Execution	4034665	Base: 5.00 Temporal: 4.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Remote Code Execution	4034681	Base: 5.00 Temporal: 4.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Remote Code Execution	4034681	Base: 5.00 Temporal: 4.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2016	4038782 (Security Update)	Important	Remote Code Execution	4034658	Base: 5.00 Temporal: 4.50	Yes

CVE-2017-8692						
					Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	
Windows Server 2016 (Server Core installation)	4038782 (Security Update)	Important	Remote Code Execution	4034658	Base: 5.00 Temporal: 4.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2017-8695 - Graphics Component Information Disclosure Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8695	**CVE Title:** Graphics Component Information Disclosure Vulnerability **Description:**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	An information disclosure vulnerability exists when Windows Uniscribe improperly discloses the contents of its memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the user'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 update addresses the vulnerability by correcting how Windows Uniscribe handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8695						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Live Meeting 2007 Add-in	4025869 (Security Update)	Important	Information Disclosure	4020736	Base: N/A Temporal: N/A Vector: N/A	Unknown
Microsoft Live Meeting 2007 Console	4025868 (Security Update)	Important	Information Disclosure	4020735	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Lync 2010 (32-bit)	4025865 (Security Update)	Important	Information Disclosure	4020732	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-8695						
Microsoft Lync 2010 (64-bit)	4025865 (Security Update)	Important	Information Disclosure	4020732	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Lync 2010 Attendee (admin level install)	4025866 (Security Update)	Important	Information Disclosure	4020733	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Lync 2010 Attendee (user level install)	4025867 (Security Update)	Important	Information Disclosure	4020734	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Lync 2013 Service Pack 1 (32-bit)	4011107 (Security Update) 3213568 (Security Update)	Important	Information Disclosure	3191939 3191937	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Lync 2013 Service	4011107 (Security Update)	Important	Information Disclosure	3191939 3191937	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-8695						
Pack 1 (64-bit)	3213568 (Security Update)					
Microsoft Lync Basic 2013 Service Pack 1 (32-bit)	4011107 (Security Update) 3213568 (Security Update)	Important	Information Disclosure	3191939 3191937	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Lync Basic 2013 Service Pack 1 (64-bit)	4011107 (Security Update) 3213568 (Security Update)	Important	Information Disclosure	3191939 3191937	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2007 Service Pack 3	3213641 (Security Update)	Important	Information Disclosure	None	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010	3213638 (Security Update)	Important	Information Disclosure	3191848	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-8695						
Service Pack 2 (32-bit editions)						
Microsoft Office 2010 Service Pack 2 (64-bit editions)	3213638 (Security Update)	Important	Information Disclosure	3191848	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office Word Viewer	4011134 (Security Update)	Important	Information Disclosure	3203484	Base: N/A Temporal: N/A Vector: N/A	Maybe
Skype for Business 2016 (32-bit)	4011040 (Security Update)	Important	Information Disclosure	3203382	Base: N/A Temporal: N/A Vector: N/A	Maybe
Skype for Business 2016 (64-bit)	4011040 (Security Update)	Important	Information Disclosure	3203382	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-8695						
Skype for Business 2016 Basic (32-bit)	4011040 (Security Update)	Important	Information Disclosure	3203382	Base: N/A Temporal: N/A Vector: N/A	Maybe
Skype for Business 2016 Basic (64-bit)	4011040 (Security Update)	Important	Information Disclosure	3203382	Base: N/A Temporal: N/A Vector: N/A	Maybe
Windows 10 for 32-bit Systems	4038781 (Security Update)	Important	Information Disclosure	4034668	Base: 7.50 Temporal: 6.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4038781 (Security Update)	Important	Information Disclosure	4034668	Base: 7.50 Temporal: 6.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4038783 (Security Update)	Important	Information Disclosure	4034660	Base: 7.50 Temporal: 6.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

CVE-2017-8695						
Windows 10 Version 1511 for x64-based Systems	4038783 (Security Update)	Important	Information Disclosure	4034660	Base: 7.50 Temporal: 6.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 7.50 Temporal: 6.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 7.50 Temporal: 6.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4038788 (Security Update)	Important	Information Disclosure	4034674	Base: 7.50 Temporal: 6.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 10 Version 1703 for	4038788 (Security Update)	Important	Information Disclosure	4034674	Base: 7.50 Temporal: 6.50 Vector:	Yes

CVE-2017-8695						
x64-based Systems					CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	
Windows 7 for 32-bit Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 7.50 Temporal: 6.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 7.50 Temporal: 6.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Information Disclosure	4034681	Base: 7.50 Temporal: 6.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows 8.1 for x64-	4038792 (Monthly Rollup)	Important	Information Disclosure	4034681	Base: 7.50 Temporal: 6.50 Vector:	Yes

CVE-2017-8695						
based systems	4038793 (Security Only)				CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	
Windows RT 8.1	4038792 (Monthly Rollup)	Important	Information Disclosure	4034681	Base: 7.50 Temporal: 6.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4039384 (Security Update)	Important	Information Disclosure	4022887	Base: 7.50 Temporal: 6.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Unknown
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server	4039384 (Security Update)	Important	Information Disclosure	4022887	Base: 7.50 Temporal: 6.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Unknown

CVE-2017-8695						
Core installation)						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4039384 (Security Update)	Important	Information Disclosure	4022887	Base: 7.50 Temporal: 6.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Unknown
Windows Server 2008 for x64-based Systems Service Pack 2	4039384 (Security Update)	Important	Information Disclosure	4022887	Base: 7.50 Temporal: 6.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Unknown
Windows Server 2008 for x64-based Systems	4039384 (Security Update)	Important	Information Disclosure	4022887	Base: 7.50 Temporal: 6.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Unknown

CVE-2017-8695						
Service Pack 2 (Server Core installation)						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 7.50 Temporal: 6.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 7.50 Temporal: 6.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

CVE-2017-8695						
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 7.50 Temporal: 6.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012	4038786 (Security Only) 4038799 (Monthly Rollup)	Important	Information Disclosure	4034665	Base: 7.50 Temporal: 6.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012 (Server Core	4038786 (Security Only) 4038799	Important	Information Disclosure	4034665	Base: 7.50 Temporal: 6.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

CVE-2017-8695						
installation)	(Monthly Rollup)					
Windows Server 2012 R2	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Information Disclosure	4034681	Base: 7.50 Temporal: 6.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Information Disclosure	4034681	Base: 7.50 Temporal: 6.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 7.50 Temporal: 6.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2016	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 7.50 Temporal: 6.50 Vector:	Yes

CVE-2017-8695						
(Server Core installation)					CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	

CVE-2017-8696 - Microsoft Graphics Component Remote Code Execution

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8696 MITRE NVD	**CVE Title:** Microsoft Graphics Component Remote Code Execution **Description:** A remote code execution vulnerability exists due to the way Windows Uniscribe 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. Users whose accounts are	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 this vulnerability: • In a web-based attack scenario, an attacker could host a specially crafted website designed to exploit this vulnerability and then convince a user 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 click a link in an email or instant message that takes users to the attacker's website, or by opening an attachment sent through email. • In a file-sharing attack scenario, an attacker could provide a specially crafted document file designed to exploit this vulnerability and then convince a user to open the document file.The security update addresses the vulnerability by correcting how Windows Uniscribe handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8696						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Live Meeting 2007 Add-in	4025869 (Security Update)	Important	Remote Code Execution	4020736	Base: N/A Temporal: N/A Vector: N/A	Unknown
Microsoft Live Meeting	4025868 (Security Update)	Important	Remote Code Execution	4020735	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-8696						
2007 Console						
Microsoft Lync 2010 (32-bit)	4025865 (Security Update)	Important	Remote Code Execution	4020732	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Lync 2010 (64-bit)	4025865 (Security Update)	Important	Remote Code Execution	4020732	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Lync 2010 Attendee (admin level install)	4025866 (Security Update)	Important	Remote Code Execution	4020733	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Lync 2010 Attendee (user level install)	4025867 (Security Update)	Important	Remote Code Execution	4020734	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Lync 2013 Service	4011107 (Security Update)	Important	Remote Code Execution	3191939	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-8696						
Pack 1 (32-bit)						
Microsoft Lync 2013 Service Pack 1 (64-bit)	4011107 (Security Update)	Important	Remote Code Execution	3191939	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Lync Basic 2013 Service Pack 1 (32-bit)	4011107 (Security Update)	Important	Remote Code Execution	3191939	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Lync Basic 2013 Service Pack 1 (64-bit)	4011107 (Security Update)	Important	Remote Code Execution	3191939	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2007 Service Pack 3	3213649 (Security Update)	Critical	Remote Code Execution	None	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-8696						
Microsoft Office 2010 Service Pack 2 (32-bit editions)	3213631 (Security Update)	Critical	Remote Code Execution	3191844	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (64-bit editions)	3213631 (Security Update)	Critical	Remote Code Execution	3191844	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office Web Apps 2010 Service Pack 2	3213632 (Security Update)	Critical	Remote Code Execution	3203466	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office Word Viewer	4011125 (Security Update)	Critical	Remote Code Execution	None	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-8696						
Skype for Business 2016 (32-bit)	4011040 (Security Update)	Important	Remote Code Execution	3203382	Base: N/A Temporal: N/A Vector: N/A	Maybe
Skype for Business 2016 (64-bit)	4011040 (Security Update)	Important	Remote Code Execution	3203382	Base: N/A Temporal: N/A Vector: N/A	Maybe
Skype for Business 2016 Basic (32-bit)	4011040 (Security Update)	Important	Remote Code Execution	3203382	Base: N/A Temporal: N/A Vector: N/A	Maybe
Skype for Business 2016 Basic (64-bit)	4011040 (Security Update)	Important	Remote Code Execution	3203382	Base: N/A Temporal: N/A Vector: N/A	Maybe
Windows 7 for 32-bit Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Critical	Remote Code Execution	4034664	Base: 7.50 Temporal: 6.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

CVE-2017-8696						
Windows 7 for x64-based Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Critical	Remote Code Execution	4034664	Base: 7.50 Temporal: 6.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4039384 (Security Update)	Critical	Remote Code Execution	4022887	Base: 7.50 Temporal: 6.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Unknown
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4039384 (Security Update)	Critical	Remote Code Execution	4022887	Base: 7.50 Temporal: 6.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Unknown

CVE-2017-8696						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4039384 (Security Update)	Critical	Remote Code Execution	4022887	Base: 7.50 Temporal: 6.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Unknown
Windows Server 2008 for x64-based Systems Service Pack 2	4039384 (Security Update)	Critical	Remote Code Execution	4022887	Base: 7.50 Temporal: 6.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Unknown
Windows Server 2008 for x64-based Systems Service Pack 2 (Server	4039384 (Security Update)	Critical	Remote Code Execution	4022887	Base: 7.50 Temporal: 6.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Unknown

CVE-2017-8696						
Core installation)						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Critical	Remote Code Execution	4034664	Base: 7.50 Temporal: 6.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Critical	Remote Code Execution	4034664	Base: 7.50 Temporal: 6.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service	4038777 (Monthly Rollup) 4038779 (Security Only)	Critical	Remote Code Execution	4034664	Base: 7.50 Temporal: 6.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Yes

CVE-2017-8696						
Pack 1 (Server Core installation)						

CVE-2017-8699 - Windows Shell Remote Code Execution Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8699 MITRE NVD	**CVE Title:** Windows Shell Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when Windows Shell does not properly validate file copy destinations. 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	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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. To exploit the vulnerability, a user must open a specially crafted file. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and then 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) that contains a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force a user to visit the website. Instead, an attacker would have to convince a user to click a link, typically by way of an enticement in an email or Instant Messenger message, and then convince the user to open the specially crafted file. The security update addresses the vulnerability by helping to ensure that Windows Shell validates file copy destinations. **FAQ:** None **Mitigations:** None **Workarounds:** None		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8699						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	4038781 (Security Update)	Important	Remote Code Execution	4034668	Base: 6.40 Temporal: 5.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4038781 (Security Update)	Important	Remote Code Execution	4034668	Base: 6.40 Temporal: 5.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8699						
Windows 10 Version 1511 for 32-bit Systems	4038783 (Security Update)	Important	Remote Code Execution	4034660	Base: 6.40 Temporal: 5.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	4038783 (Security Update)	Important	Remote Code Execution	4034660	Base: 6.40 Temporal: 5.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4038782 (Security Update)	Important	Remote Code Execution	4034658	Base: 6.40 Temporal: 5.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4038782 (Security Update)	Important	Remote Code Execution	4034658	Base: 6.40 Temporal: 5.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for	4038788 (Security Update)	Important	Remote Code Execution	4034674	Base: 6.40 Temporal: 5.80	Yes

CVE-2017-8699						
32-bit Systems					Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1703 for x64-based Systems	4038788 (Security Update)	Important	Remote Code Execution	4034674	Base: 6.40 Temporal: 5.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for 32-bit Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Remote Code Execution	4034664	Base: 6.40 Temporal: 5.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Remote Code Execution	4034664	Base: 6.40 Temporal: 5.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4038792 (Monthly Rollup) 4038793	Important	Remote Code Execution	4034681	Base: 6.40 Temporal: 5.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8699						
	(Security Only)					
Windows 8.1 for x64-based systems	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Remote Code Execution	4034681	Base: 6.40 Temporal: 5.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4038792 (Monthly Rollup)	Important	Remote Code Execution	4034681	Base: 6.40 Temporal: 5.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4039266 (Security Update)	Important	Remote Code Execution	4021903	Base: 6.40 Temporal: 5.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit	4039266 (Security Update)	Important	Remote Code Execution	4021903	Base: 6.40 Temporal: 5.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8699						
Systems Service Pack 2 (Server Core installation)						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4039266 (Security Update)	Important	Remote Code Execution	4021903	Base: 6.40 Temporal: 5.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4039266 (Security Update)	Important	Remote Code Execution	4021903	Base: 6.40 Temporal: 5.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8699						
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4039266 (Security Update)	Important	Remote Code Execution	4021903	Base: 6.40 Temporal: 5.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Remote Code Execution	4034664	Base: 6.40 Temporal: 5.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Remote Code Execution	4034664	Base: 6.40 Temporal: 5.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8699						
Pack 1 (Server Core installation)						
Windows Server 2012	4038786 (Security Only) 4038799 (Monthly Rollup)	Important	Remote Code Execution	4034665	Base: 6.40 Temporal: 5.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4038786 (Security Only) 4038799 (Monthly Rollup)	Important	Remote Code Execution	4034665	Base: 6.40 Temporal: 5.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Remote Code Execution	4034681	Base: 6.40 Temporal: 5.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8699						
Windows Server 2012 R2 (Server Core installation)	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Remote Code Execution	4034681	Base: 6.40 Temporal: 5.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4038782 (Security Update)	Important	Remote Code Execution	4034658	Base: 6.40 Temporal: 5.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4038782 (Security Update)	Important	Remote Code Execution	4034658	Base: 6.40 Temporal: 5.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8702 - Windows Elevation of Privilege Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8702 MITRE NVD	**CVE Title:** Windows Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files. The vulnerability could allow elevation of privilege if an attacker can successfully exploit it. An attacker who successfully exploited the vulnerability could gain greater access to sensitive information and system functionality. To exploit the vulnerability, an attacker could run a specially crafted application. The security update addresses the vulnerability by correcting the way that WER handles and executes files. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information published.	Important	Elevation of Privilege

Affected Software

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

CVE-2017-8702						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	4038781 (Security Update)	Important	Elevation of Privilege	4034668	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4038781 (Security Update)	Important	Elevation of Privilege	4034668	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4038783 (Security Update)	Important	Elevation of Privilege	4034660	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for	4038783 (Security Update)	Important	Elevation of Privilege	4034660	Base: 7.50 Temporal: 6.70	Yes

CVE-2017-8702						
x64-based Systems					Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1607 for 32-bit Systems	4038782 (Security Update)	Important	Elevation of Privilege	4034658	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4038782 (Security Update)	Important	Elevation of Privilege	4034658	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4038782 (Security Update)	Important	Elevation of Privilege	4034658	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4038782 (Security Update)	Important	Elevation of Privilege	4034658	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8704 - Hyper-V Denial of Service Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8704 MITRE NVD	**CVE Title:** Hyper-V Denial of Service Vulnerability **Description:** A denial of service vulnerability exists when Microsoft Hyper-V Virtual PCI 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 properly validating input. **FAQ:** None **Mitigations:** None **Workarounds:** None	Important	Denial of Service

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8704						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1607 for x64-based Systems	4038782 (Security Update)	Important	Denial of Service	4034658	Base: 5.30 Temporal: 4.80 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4038782 (Security Update)	Important	Denial of Service	4034658	Base: 5.30 Temporal: 4.80 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8704						
Windows Server 2016 (Server Core installation)	4038782 (Security Update)	Important	Denial of Service	4034658	Base: 5.30 Temporal: 4.80 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8706 - Hyper-V Information Disclosure Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8706 MITRE NVD	**CVE Title:** Hyper-V Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when Windows Hyper-V on a host operating system fails to properly validate input from an authenticated user on a guest operating system. To exploit the vulnerability, an attacker on a guest operating system could run a specially crafted application that could cause the Hyper-V host operating system to disclose memory information. An attacker who successfully exploited the vulnerability could gain access to information on the Hyper-V host operating system.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by correcting how Hyper-V validates guest operating system user input. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8706						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for x64-based Systems	4038781 (Security Update)	Important	Information Disclosure	4034668	Base: 7.20 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	4038783 (Security Update)	Important	Information Disclosure	4034660	Base: 7.20 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 7.20 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4038788 (Security Update)	Important	Information Disclosure	4034674	Base: 7.20 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8706						
Windows Server 2016	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 7.20 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 7.20 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8707 - Hyper-V Information Disclosure Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8707 MITRE NVD	**CVE Title:** Hyper-V Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when Windows Hyper-V on a host operating system fails to properly validate input from an authenticated user on a guest operating system. To exploit the vulnerability, an attacker on a guest operating system could run a specially crafted application that could cause the Hyper-V host operating system to disclose memory information. An attacker who successfully exploited the vulnerability could gain access to information on the Hyper-V host operating system. The security update addresses the vulnerability by correcting how Hyper-V validates guest operating system user input. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information published. 1.1 2017-09-12T07:00:00 Added Windows Server 2012 and Windows Server 2012	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	(Server Core Installation) as affected by CVE-2017-8707. This is an informational change only.		

Affected Software

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

CVE-2017-8707						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for x64-based Systems	4038781 (Security Update)	Important	Information Disclosure	4034668	Base: 7.20 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for	4038783 (Security Update)	Important	Information Disclosure	4034660	Base: 7.20 Temporal: 6.50 Vector:	Yes

CVE-2017-8707						
x64-based Systems					CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1607 for x64-based Systems	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 7.20 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4038788 (Security Update)	Important	Information Disclosure	4034674	Base: 7.20 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Information Disclosure	4034681	Base: 7.20 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems	4039325 (Security Update)	Important	Information Disclosure	None	Base: 7.20 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8707						
Service Pack 2						
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4039325 (Security Update)	Important	Information Disclosure	None	Base: 7.20 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 7.20 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8707						
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 7.20 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012	4038786 (Security Only) 4038799 (Monthly Rollup)	Important	Information Disclosure	4034665	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2012 (Server Core	4038786 (Security Only) 4038799	Important	Information Disclosure	4034665	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2017-8707						
installation)	(Monthly Rollup)					
Windows Server 2012 R2	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Information Disclosure	4034681	Base: 7.20 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Information Disclosure	4034681	Base: 7.20 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 7.20 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 7.20 Temporal: 6.50 Vector:	Yes

CVE-2017-8707						
(Server Core installation)					CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C	

CVE-2017-8708 - Windows Kernel Information Disclosure Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8708 MITRE NVD	**CVE Title:** Windows Kernel Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the Windows kernel fails to properly initialize a memory address, allowing an attacker to retrieve information that could lead to a Kernel Address Space Layout Randomization (KASLR) bypass. An attacker who successfully exploited this vulnerability could retrieve the base address of the kernel driver from a compromised process. 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 the Windows kernel handles memory addresses. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.1 2017-09-12T07:00:00 Updated acknowledgment. This is an informational change only. 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8708						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	4038781 (Security Update)	Important	Information Disclosure	4034668	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4038781 (Security Update)	Important	Information Disclosure	4034668	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4038783 (Security Update)	Important	Information Disclosure	4034660	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	4038783 (Security Update)	Important	Information Disclosure	4034660	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8708						
Windows 10 Version 1607 for 32-bit Systems	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4038788 (Security Update)	Important	Information Disclosure	4034674	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4038788 (Security Update)	Important	Information Disclosure	4034674	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 7 for 32-bit Systems	4038777 (Monthly Rollup)	Important	Information Disclosure	4034664	Base: 4.70 Temporal: 4.20 Vector:	Yes

CVE-2017-8708						
Service Pack 1	4038779 (Security Only)				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 7 for x64-based Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Information Disclosure	4034681	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Information Disclosure	4034681	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8708						
Windows RT 8.1	4038792 (Monthly Rollup)	Important	Information Disclosure	4034681	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4038874 (Security Update)	Important	Information Disclosure	4022013	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4038874 (Security Update)	Important	Information Disclosure	4022013	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown

CVE-2017-8708						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4038874 (Security Update)	Important	Information Disclosure	4022013	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for x64-based Systems Service Pack 2	4038874 (Security Update)	Important	Information Disclosure	4022013	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for x64-based Systems Service Pack 2 (Server	4038874 (Security Update)	Important	Information Disclosure	4022013	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown

CVE-2017-8708						
Core installation)						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2	4038777 (Monthly Rollup)	Important	Information Disclosure	4034664	Base: 4.70 Temporal: 4.20 Vector:	Yes

CVE-2017-8708						
for x64-based Systems Service Pack 1 (Server Core installation)	4038779 (Security Only)				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2012	4038786 (Security Only) 4038799 (Monthly Rollup)	Important	Information Disclosure	4034665	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4038786 (Security Only) 4038799 (Monthly Rollup)	Important	Information Disclosure	4034665	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8708						
Windows Server 2012 R2	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Information Disclosure	4034681	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Information Disclosure	4034681	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8708						
installation)						

CVE-2017-8709 - Windows Kernel Information Disclosure Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8709 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 user'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.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8709						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2017-8709						
Windows 10 for 32-bit Systems	4038781 (Security Update)	Important	Information Disclosure	4034668	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4038781 (Security Update)	Important	Information Disclosure	4034668	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4038783 (Security Update)	Important	Information Disclosure	4034660	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	4038783 (Security Update)	Important	Information Disclosure	4034660	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 4.70 Temporal: 4.20 Vector:	Yes

CVE-2017-8709						
32-bit Systems					CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1607 for x64-based Systems	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4038788 (Security Update)	Important	Information Disclosure	4034674	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4038788 (Security Update)	Important	Information Disclosure	4034674	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 7 for 32-bit Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8709						
Windows 7 for x64-based Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Information Disclosure	4034681	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Information Disclosure	4034681	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4038792 (Monthly Rollup)	Important	Information Disclosure	4034681	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8709						
Windows Server 2008 for 32-bit Systems Service Pack 2	4032201 (Security Update)	Important	Information Disclosure	None	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4032201 (Security Update)	Important	Information Disclosure	None	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based	4032201 (Security Update)	Important	Information Disclosure	None	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8709						
Systems Service Pack 2						
Windows Server 2008 for x64-based Systems Service Pack 2	4032201 (Security Update)	Important	Information Disclosure	None	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4032201 (Security Update)	Important	Information Disclosure	None	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8709						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8709						
Service Pack 1 (Server Core installation)						
Windows Server 2012	4038786 (Security Only) 4038799 (Monthly Rollup)	Important	Information Disclosure	4034665	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4038786 (Security Only) 4038799 (Monthly Rollup)	Important	Information Disclosure	4034665	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4038792 (Monthly Rollup) 4038793	Important	Information Disclosure	4034681	Base: 4.70 Temporal: 4.20 Vector:	Yes

CVE-2017-8709						
	(Security Only)				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2012 R2 (Server Core installation)	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Information Disclosure	4034681	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8710 - Windows Information Disclosure Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8710 MITRE NVD	**CVE Title:** Windows Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists in the Microsoft Common Console Document (.msc) when it improperly parses XML input containing a reference to an external entity. 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 a file containing specially crafted XML content and convince an authenticated user to open the file. The update addresses the vulnerability by modifying the way that the Microsoft Common Console Document (.msc) parses XML input. **FAQ:** None **Mitigations:** None **Workarounds:** None	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.1 2017-09-12T07:00:00 Corrected the affected Windows component in the CVE description. This is an informational change only. 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8710						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 4.40 Temporal: 4.00 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8710						
Windows 7 for x64-based Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 4.40 Temporal: 4.00 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/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	4039038 (Security Update)	Important	Information Disclosure	None	Base: 4.40 Temporal: 4.00 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/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	4039038 (Security Update)	Important	Information Disclosure	None	Base: 4.40 Temporal: 4.00 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8710						
installation)						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4039038 (Security Update)	Important	Information Disclosure	None	Base: 4.40 Temporal: 4.00 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/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	4039038 (Security Update)	Important	Information Disclosure	None	Base: 4.40 Temporal: 4.00 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service	4039038 (Security Update)	Important	Information Disclosure	None	Base: 4.40 Temporal: 4.00 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8710						
Pack 2 (Server Core installation)						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 4.40 Temporal: 4.00 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/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	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 4.40 Temporal: 4.00 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8710						
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 4.40 Temporal: 4.00 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8711 - Hyper-V Information Disclosure Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8711 MITRE NVD	**CVE Title:** Hyper-V Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when Windows Hyper-V on a host operating system fails to properly validate input from an authenticated user on a guest operating system. To exploit the vulnerability, an attacker on a guest operating system could run a specially crafted application that could cause the Hyper-V host operating system to disclose memory information. An attacker who successfully exploited the vulnerability could gain access to information on the Hyper-V host operating system. The security update addresses the vulnerability by correcting how Hyper-V validates guest operating system user input. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information published.	Important	Information Disclosure

Affected Software

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

CVE-2017-8711						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1607 for x64-based Systems	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 7.20 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 7.20 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 7.20 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8711						
installation)						

CVE-2017-8712 - Hyper-V Information Disclosure Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8712 MITRE NVD	**CVE Title:** Hyper-V Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when Windows Hyper-V on a host operating system fails to properly validate input from an authenticated user on a guest operating system. To exploit the vulnerability, an attacker on a guest operating system could run a specially crafted application that could cause the Hyper-V host operating system to disclose memory information. An attacker who successfully exploited the vulnerability could gain access to information on the Hyper-V host operating system. The security update addresses the vulnerability by correcting how Hyper-V validates guest operating system user input.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8712						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2017-8712						
Windows 10 Version 1607 for x64-based Systems	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 7.20 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4038788 (Security Update)	Important	Information Disclosure	4034674	Base: 7.20 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 7.20 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 7.20 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8713 - Hyper-V Information Disclosure Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8713 MITRE NVD	**CVE Title:** Hyper-V Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when Windows Hyper-V on a host operating system fails to properly validate input from an authenticated user on a guest operating system. To exploit the vulnerability, an attacker on a guest operating system could run a specially crafted application that could cause the Hyper-V host operating system to disclose memory information. An attacker who successfully exploited the vulnerability could gain access to information on the Hyper-V host operating system. The security update addresses the vulnerability by correcting how Hyper-V validates guest operating system user input. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8713						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for x64-based Systems	4038781 (Security Update)	Important	Information Disclosure	4034668	Base: 7.20 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8713						
Windows 10 Version 1511 for x64-based Systems	4038783 (Security Update)	Important	Information Disclosure	4034660	Base: 7.20 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 7.20 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4038788 (Security Update)	Important	Information Disclosure	4034674	Base: 7.20 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Information Disclosure	4034681	Base: 7.20 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8713						
Windows Server 2012	4038786 (Security Only) 4038799 (Monthly Rollup)	Important	Information Disclosure	4034665	Base: 7.20 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4038786 (Security Only) 4038799 (Monthly Rollup)	Important	Information Disclosure	4034665	Base: 7.20 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Information Disclosure	4034681	Base: 7.20 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server	4038792 (Monthly Rollup) 4038793	Important	Information Disclosure	4034681	Base: 7.20 Temporal: 6.50 Vector:	Yes

CVE-2017-8713						
Core installation)	(Security Only)				CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C	
Windows Server 2016	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 7.20 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 7.20 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8714 - Remote Desktop Virtual Host Remote Code Execution Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8714 MITRE NVD	**CVE Title:** Remote Desktop Virtual Host Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in the VM Host Agent Service of Remote Desktop Virtual Host role when it fails to properly validate input from an authenticated user on a guest operating system. To exploit the vulnerability, an attacker could issue a specially crafted certificate on the guest operating system that could cause the VM host agent service on the host operating system to execute arbitrary code. The Remote Desktop Virtual Host role is not enabled by default. An attacker who successfully exploited the vulnerability could execute arbitrary code on the host operating system. The security update addresses the vulnerability by correcting how VM host agent service validates guest operating system user input. **FAQ:** None	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information published. 1.1 2017-09-12T07:00:00 Removed Windows 10 for x64-based Systems as affected by CVE-2017-8714. This is an informational change only.		

Affected Software

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

CVE-2017-8714						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1607 for	4038782 (Security Update)	Important	Remote Code Execution	4034658	Base: 7.80 Temporal: 7.00	Yes

CVE-2017-8714						
x64-based Systems					Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 8.1 for x64-based systems	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Remote Code Execution	4034681	Base: 7.80 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012	4038786 (Security Only) 4038799 (Monthly Rollup)	Important	Remote Code Execution	4034665	Base: 7.80 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4038786 (Security Only) 4038799 (Monthly Rollup)	Important	Remote Code Execution	4034665	Base: 7.80 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4038792 (Monthly Rollup)	Important	Remote Code Execution	4034681	Base: 7.80 Temporal: 7.00	Yes

CVE-2017-8714						
	4038793 (Security Only)				Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2012 R2 (Server Core installation)	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Remote Code Execution	4034681	Base: 7.80 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4038782 (Security Update)	Important	Remote Code Execution	4034658	Base: 7.80 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4038782 (Security Update)	Important	Remote Code Execution	4034658	Base: 7.80 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8716 - Windows Security Feature Bypass Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8716 MITRE NVD	**CVE Title:** Windows Security Feature Bypass Vulnerability **Description:** A security feature bypass vulnerability exists when Windows Control Flow Guard mishandles objects in memory. To exploit the vulnerability, an attacker could run a specially crafted application to bypass Control Flow Guard. The security update addresses the vulnerability by correcting how Windows Control Flow Guard handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information published.	Important	Security Feature Bypass

Affected Software

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

CVE-2017-8716						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1703 for 32-bit Systems	4038788 (Security Update)	Important	Security Feature Bypass	4034674	Base: 4.90 Temporal: 4.40 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4038788 (Security Update)	Important	Security Feature Bypass	4034674	Base: 4.90 Temporal: 4.40 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2017-8719 - Windows Kernel Information Disclosure Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8719 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 user'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:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information Published.	Important	Information Disclosure

Affected Software

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

CVE-2017-8719						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	4038781 (Security Update)	Important	Information Disclosure	4034668	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4038781 (Security Update)	Important	Information Disclosure	4034668	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4038783 (Security Update)	Important	Information Disclosure	4034660	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8719						
Windows 10 Version 1511 for x64-based Systems	4038783 (Security Update)	Important	Information Disclosure	4034660	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4038788 (Security Update)	Important	Information Disclosure	4034674	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for	4038788 (Security Update)	Important	Information Disclosure	4034674	Base: 4.70 Temporal: 4.20 Vector:	Yes

CVE-2017-8719						
x64-based Systems					CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 8.1 for 32-bit systems	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Information Disclosure	4034681	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Information Disclosure	4034681	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4038792 (Monthly Rollup)	Important	Information Disclosure	4034681	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit	4038874 (Security Update)	Important	Information Disclosure	4022013	Base: 4.70 Temporal: 4.20 Vector:	Unknown

CVE-2017-8719						
Systems Service Pack 2					CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4038874 (Security Update)	Important	Information Disclosure	4022013	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4038874 (Security Update)	Important	Information Disclosure	4022013	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown

CVE-2017-8719						
Windows Server 2008 for x64-based Systems Service Pack 2	4038874 (Security Update)	Important	Information Disclosure	4022013	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4038874 (Security Update)	Important	Information Disclosure	4022013	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 R2 for Itanium-	4038777 (Monthly Rollup) 4038779	Important	Information Disclosure	4034664	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8719						
Based Systems Service Pack 1	(Security Only)					
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Information Disclosure	4034664	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8719						
installation)						
Windows Server 2012	4038786 (Security Only) 4038799 (Monthly Rollup)	Important	Information Disclosure	4034665	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4038786 (Security Only) 4038799 (Monthly Rollup)	Important	Information Disclosure	4034665	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Information Disclosure	4034681	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8719						
Windows Server 2012 R2 (Server Core installation)	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Information Disclosure	4034681	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8720 - Win32k Elevation of Privilege Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8720 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. 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:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8720						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	4038781 (Security Update)	Important	Elevation of Privilege	4034668	Base: 7.80 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4038781 (Security Update)	Important	Elevation of Privilege	4034668	Base: 7.80 Temporal: 7.00 Vector: CVSS: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-2017-8720						
Windows 10 Version 1511 for 32-bit Systems	4038783 (Security Update)	Important	Elevation of Privilege	4034660	Base: 7.80 Temporal: 7.00 Vector: CVSS: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 1511 for x64-based Systems	4038783 (Security Update)	Important	Elevation of Privilege	4034660	Base: 7.80 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4038782 (Security Update)	Important	Elevation of Privilege	4034658	Base: 7.80 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4038782 (Security Update)	Important	Elevation of Privilege	4034658	Base: 7.80 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for	4038788 (Security Update)	Important	Elevation of Privilege	4034674	Base: 7.80 Temporal: 7.00	Yes

CVE-2017-8720						
32-bit 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 1703 for x64-based Systems	4038788 (Security Update)	Important	Elevation of Privilege	4034674	Base: 7.80 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for 32-bit Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Elevation of Privilege	4034664	Base: 7.80 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Elevation of Privilege	4034664	Base: 7.80 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4038792 (Monthly Rollup) 4038793	Important	Elevation of Privilege	4034681	Base: 7.80 Temporal: 7.00 Vector: CVSS: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-2017-8720						
	(Security Only)					
Windows 8.1 for x64-based systems	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Elevation of Privilege	4034681	Base: 7.80 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4038792 (Monthly Rollup)	Important	Elevation of Privilege	4034681	Base: 7.80 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4039384 (Security Update)	Important	Elevation of Privilege	4022887	Base: 7.80 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for 32-bit Systems Service	4039384 (Security Update)	Important	Elevation of Privilege	4022887	Base: 7.80 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2017-8720						
Pack 2 (Server Core installation)						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4039384 (Security Update)	Important	Elevation of Privilege	4022887	Base: 7.80 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for x64-based Systems Service Pack 2	4039384 (Security Update)	Important	Elevation of Privilege	4022887	Base: 7.80 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for x64-based Systems	4039384 (Security Update)	Important	Elevation of Privilege	4022887	Base: 7.80 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2017-8720						
Service Pack 2 (Server Core installation)						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Elevation of Privilege	4034664	Base: 7.80 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4038777 (Monthly Rollup) 4038779 (Security Only)	Important	Elevation of Privilege	4034664	Base: 7.80 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-	4038777 (Monthly Rollup)	Important	Elevation of Privilege	4034664	Base: 7.80 Temporal: 7.00	Yes

CVE-2017-8720						
based Systems Service Pack 1 (Server Core installation)	4038779 (Security Only)				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2012	4038786 (Security Only) 4038799 (Monthly Rollup)	Important	Elevation of Privilege	4034665	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2012 (Server Core installation)	4038786 (Security Only) 4038799 (Monthly Rollup)	Important	Elevation of Privilege	4034665	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2012 R2	4038792 (Monthly Rollup) 4038793	Important	Elevation of Privilege	4034681	Base: 7.80 Temporal: 7.00 Vector: CVSS: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-2017-8720						
	(Security Only)					
Windows Server 2012 R2 (Server Core installation)	4038792 (Monthly Rollup) 4038793 (Security Only)	Important	Elevation of Privilege	4034681	Base: 7.80 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4038782 (Security Update)	Important	Elevation of Privilege	4034658	Base: 7.80 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4038782 (Security Update)	Important	Elevation of Privilege	4034658	Base: 7.80 Temporal: 7.00 Vector: CVSS: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-2017-8723 - Microsoft Edge Security Feature Bypass Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8723 MITRE NVD	**CVE Title:** Microsoft Edge Security Feature Bypass Vulnerability **Description:** A security feature bypass exists in Microsoft Edge when the Edge Content Security Policy (CSP) fails to properly validate certain specially crafted documents. An attacker who exploited the bypass could trick a user into loading a page containing malicious content. To exploit the bypass, an attacker must trick a user into either loading a page containing malicious content or visiting a malicious website. The attacker could also inject the malicious page into either a compromised website or an advertisement network. The update addresses the bypass by correcting how the Edge CSP validates documents. **FAQ:** None **Mitigations:** None **Workarounds:**	Moderate	Security Feature Bypass

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8723						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4038781 (Security Update)	Moderate	Security Feature Bypass	4034668	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows	4038781 (Security Update)	Moderate	Security Feature Bypass	4034668	Base: 4.30 Temporal: 3.90	Yes

CVE-2017-8723						
10 for x64-based Systems					Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems	4038783 (Security Update)	Moderate	Security Feature Bypass	4034660	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1511 for x64-based Systems	4038783 (Security Update)	Moderate	Security Feature Bypass	4034660	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1607 for	4038782 (Security Update)	Moderate	Security Feature Bypass	4034658	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8723						
32-bit Systems						
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4038782 (Security Update)	Moderate	Security Feature Bypass	4034658	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4038788 (Security Update)	Moderate	Security Feature Bypass	4034674	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4038788 (Security Update)	Moderate	Security Feature Bypass	4034674	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8723						
Microsoft Edge on Windows Server 2016	4038782 (Security Update)	Low	Security Feature Bypass	4034658	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8724 - Microsoft Edge Spoofing Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8724 MITRE NVD	**CVE Title:** Microsoft Edge Spoofing Vulnerability **Description:** A spoofing vulnerability exists when Microsoft Edge does not properly parse HTTP content. An attacker who successfully exploited this vulnerability could trick a user by redirecting the user to a specially crafted website. The specially crafted website could either spoof content or serve as a pivot to chain an attack with other vulnerabilities in web services.	Important	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	To exploit the vulnerability, the user must click a specially crafted URL. In an email attack scenario, an attacker could send an email message containing the specially crafted URL to the user in an attempt to convince the user to click it. In a web-based attack scenario, an attacker could host a specially crafted website designed to appear as a legitimate website to the user. However, the attacker would have no way to force the user to visit the specially crafted website. The attacker would have to convince the user to visit the specially crafted website, typically by way of enticement in an email or instant message, and then convince the user to interact with content on the website. The update addresses the vulnerability by correcting how Microsoft Edge parses HTTP responses. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8724						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4038788 (Security Update)	Important	Spoofing	4034674	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4038788 (Security Update)	Important	Spoofing	4034674	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8728 - Microsoft PDF Remote Code Execution Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8728 MITRE NVD	**CVE Title:** Microsoft PDF Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when Microsoft Windows PDF Library improperly handles objects in memory. The vulnerability could corrupt memory in a way that enables an attacker to execute arbitrary code in the context of the current user. 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 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. To exploit the vulnerability on Windows 10 systems with Microsoft Edge set as the default browser, an attacker could host a specially crafted website that contains malicious PDF content and then convince users 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 PDF content to such sites. Only Windows 10 systems with Microsoft Edge set as the default browser can be compromised simply by viewing a website. The browsers for all other affected operating systems do not automatically render PDF content, so an attacker would have no way to	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	force users to view attacker-controlled content. Instead, an attacker would have to convince users to open a specially crafted PDF document, typically by way of an enticement in an email or instant message or by way of an email attachment. The update addresses the vulnerability by modifying how affected systems handle objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8728						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4038781 (Security Update)	Critical	Remote Code Execution	4034668	Base: 4.20 Temporal: 3.80 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	4038781 (Security Update)	Critical	Remote Code Execution	4034668	Base: 4.20 Temporal: 3.80 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 1511 for 32-bit Systems	4038783 (Security Update)	Critical	Remote Code Execution	4034660	Base: 4.20 Temporal: 3.80 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	4038783 (Security Update)	Critical	Remote Code Execution	4034660	Base: 4.20 Temporal: 3.80	Yes

CVE-2017-8728						
10 Version 1511 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 1607 for 32-bit Systems	4038782 (Security Update)	Critical	Remote Code Execution	4034658	Base: 4.20 Temporal: 3.80 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	4038782 (Security Update)	Critical	Remote Code Execution	4034658	Base: 4.20 Temporal: 3.80 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	4038788 (Security Update)	Critical	Remote Code Execution	4034674	Base: 4.20 Temporal: 3.80 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-2017-8728						
32-bit Systems						
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4038788 (Security Update)	Critical	Remote Code Execution	4034674	Base: 4.20 Temporal: 3.80 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	4038782 (Security Update)	Moderate	Remote Code Execution	4034658	Base: 4.20 Temporal: 3.80 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
Windows 8.1 for 32-bit systems	4038792 (Monthly Rollup) 4038793 (Security Only)	Critical	Remote Code Execution	4034681	Base: 4.20 Temporal: 3.80 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
Windows 8.1 for x64-	4038792 (Monthly Rollup)	Critical	Remote Code Execution	4034681	Base: 4.20 Temporal: 3.80	Yes

CVE-2017-8728						
based systems	4038793 (Security Only)				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	
Windows RT 8.1	4038792 (Monthly Rollup)	Critical	Remote Code Execution	4034681	Base: 4.20 Temporal: 3.80 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
Windows Server 2012	4038786 (Security Only) 4038799 (Monthly Rollup)	Critical	Remote Code Execution	4034665	Base: 4.20 Temporal: 3.80 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
Windows Server 2012 (Server Core installation)	4038786 (Security Only) 4038799 (Monthly Rollup)	Critical	Remote Code Execution	4034665	Base: 4.20 Temporal: 3.80 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
Windows Server 2012 R2	4038792 (Monthly Rollup) 4038793	Critical	Remote Code Execution	4034681	Base: 4.20 Temporal: 3.80 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-2017-8728						
	(Security Only)					
Windows Server 2012 R2 (Server Core installation)	4038792 (Monthly Rollup) 4038793 (Security Only)	Critical	Remote Code Execution	4034681	Base: 4.20 Temporal: 3.80 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-2017-8729 - Scripting Engine Memory Corruption Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8729 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 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	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 update addresses the vulnerability by modifying how the scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8729						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4038788 (Security Update)	Critical	Remote Code Execution	4034674	Base: 4.20 Temporal: 3.80 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	4038788 (Security Update)	Critical	Remote Code Execution	4034674	Base: 4.20 Temporal: 3.80 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-2017-8731 - Microsoft Edge Memory Corruption Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8731 MITRE NVD	**CVE Title:** Microsoft Edge Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory. The vulnerability could corrupt memory in such a way that enables 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, an 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 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 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 by way of enticement in an email or Instant Messenger message, or by getting them 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 Microsoft Edge handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8731						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2017-8731						
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4038782 (Security Update)	Critical	Remote Code Execution	4034658	Base: 4.20 Temporal: 3.80 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	4038782 (Security Update)	Critical	Remote Code Execution	4034658	Base: 4.20 Temporal: 3.80 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	4038782 (Security Update)	Moderate	Remote Code Execution	4034658	Base: 3.10 Temporal: 2.80 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8733 - Internet Explorer Spoofing Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8733 MITRE NVD	**CVE Title:** Internet Explorer Spoofing Vulnerability **Description:** A spoofing vulnerability exists when Internet Explorer improperly handles specific HTML content. An attacker who successfully exploited this vulnerability could trick a user into believing that the user was visiting a legitimate website. The specially crafted website could either spoof content or serve as a pivot to chain an attack with other vulnerabilities in web services. To exploit the vulnerability, the user must either browse to a malicious website or be redirected to it. In an email attack scenario, an attacker could send an email message in an attempt to convince the user to click a link to the malicious website. In a web-based attack scenario, an attacker could host a specially crafted website designed to appear as a legitimate website to the user. However, the attacker would have no way to force the user to visit the specially crafted website. The attacker would have to convince the user to visit the specially crafted website, typically by way of enticement in an email or instant message. The security update addresses the vulnerability by correcting how Internet Explorer handles specific HTML content.	Important	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8733						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer	4038799 (Monthly	Low	Spoofing	4034665 4034733	Base: 2.40 Temporal: 2.20	Yes

CVE-2017-8733						
10 on Windows Server 2012	Rollup) 4036586 (IE Cumulative)				Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	
Internet Explorer 11 on Windows 10 for 32-bit Systems	4038781 (Security Update)	Important	Spoofing	4034668	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 for x64-based Systems	4038781 (Security Update)	Important	Spoofing	4034668	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows	4038783 (Security Update)	Important	Spoofing	4034660	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8733						
10 Version 1511 for 32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1511 for x64-based Systems	4038783 (Security Update)	Important	Spoofing	4034660	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1607 for	4038782 (Security Update)	Important	Spoofing	4034658	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8733						
32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4038782 (Security Update)	Important	Spoofing	4034658	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems	4038788 (Security Update)	Important	Spoofing	4034674	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8733						
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems	4038788 (Security Update)	Important	Spoofing	4034674	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1	4038777 (Monthly Rollup) 4036586 (IE Cumulative)	Important	Spoofing	4034664 4034733	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows	4038777 (Monthly Rollup)	Important	Spoofing	4034664 4034733	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8733						
7 for x64-based Systems Service Pack 1	4036586 (IE Cumulative)					
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4038792 (Monthly Rollup) 4036586 (IE Cumulative)	Important	Spoofing	4034681 4034733	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 8.1 for x64-based systems	4038792 (Monthly Rollup) 4036586 (IE Cumulative)	Important	Spoofing	4034681 4034733	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8733						
Internet Explorer 11 on Windows RT 8.1	4038792 (Monthly Rollup)	Important	Spoofing	4034681	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4038777 (Monthly Rollup) 4036586 (IE Cumulative)	Low	Spoofing	4034664 4034733	Base: 2.40 Temporal: 2.20 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2012 R2	4038792 (Monthly Rollup) 4036586 (IE Cumulative)	Low	Spoofing	4034681 4034733	Base: 2.40 Temporal: 2.20 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8733						
Internet Explorer 11 on Windows Server 2016	4038782 (Security Update)	Low	Spoofing	4034658	Base: 2.40 Temporal: 2.20 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2	4036586 (IE Cumulative)	Low	Spoofing	4034733	Base: 2.40 Temporal: 2.20 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 9 on Windows Server 2008 for x64-	4036586 (IE Cumulative)	Low	Spoofing	4034733	Base: 2.40 Temporal: 2.20 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8733						
based Systems Service Pack 2						

CVE-2017-8734 - Microsoft Edge Memory Corruption Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8734 MITRE NVD	**CVE Title:** Microsoft Edge Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory. The vulnerability could corrupt memory in such a way that enables 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, an 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.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 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 by way of enticement in an email or Instant Messenger message, or by getting them to open an attachment sent through email. The security update addresses the vulnerability by modifying how Microsoft Edge handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8734						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4038781 (Security Update)	Critical	Remote Code Execution	4034668	Base: 4.20 Temporal: 3.80 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	4038781 (Security Update)	Critical	Remote Code Execution	4034668	Base: 4.20 Temporal: 3.80 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 1511 for	4038783 (Security Update)	Critical	Remote Code Execution	4034660	Base: 4.20 Temporal: 3.80 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-2017-8734						
32-bit Systems						
Microsoft Edge on Windows 10 Version 1511 for x64-based Systems	4038783 (Security Update)	Critical	Remote Code Execution	4034660	Base: 4.20 Temporal: 3.80 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	4038782 (Security Update)	Critical	Remote Code Execution	4034658	Base: 4.20 Temporal: 3.80 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	4038782 (Security Update)	Critical	Remote Code Execution	4034658	Base: 4.20 Temporal: 3.80 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-2017-8734						
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4038788 (Security Update)	Critical	Remote Code Execution	4034674	Base: 4.20 Temporal: 3.80 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	4038788 (Security Update)	Critical	Remote Code Execution	4034674	Base: 4.20 Temporal: 3.80 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	4038782 (Security Update)	Moderate	Remote Code Execution	4034658	Base: 3.10 Temporal: 2.80 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8736 - Microsoft Browser Information Disclosure Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8736 MITRE NVD	**CVE Title:** Microsoft Browser Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists in Microsoft browsers due to improper parent domain verification in certain functionality. An attacker who successfully exploited the vulnerability could obtain specific information that is used in the parent domain. To exploit the vulnerability, an attacker must have access to host malicious content on a website this is on a subdomain of the parent domain, and then convince a user to visit the site. The security update addresses the vulnerability by helping to ensure that Microsoft browsers restrict access to certain functionality between the subdomain and the parent domain. **FAQ:** None	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8736						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 11 on Windows	4038781 (Security Update)	Important	Information Disclosure	4034668	Base: 4.30 Temporal: 3.90 Vector:	Yes

CVE-2017-8736						
10 for 32-bit Systems					CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	
Internet Explorer 11 on Windows 10 for x64-based Systems	4038781 (Security Update)	Important	Information Disclosure	4034668	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1511 for 32-bit Systems	4038783 (Security Update)	Important	Information Disclosure	4034660	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on	4038783 (Security Update)	Important	Information Disclosure	4034660	Base: 4.30 Temporal: 3.90 Vector:	Yes

CVE-2017-8736						
Windows 10 Version 1511 for x64-based Systems					CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1607 for	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8736						
x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems	4038788 (Security Update)	Important	Information Disclosure	4034674	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems	4038788 (Security Update)	Important	Information Disclosure	4034674	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8736						
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1	4038777 (Monthly Rollup) 4036586 (IE Cumulative)	Important	Information Disclosure	4034664 4034733	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1	4038777 (Monthly Rollup) 4036586 (IE Cumulative)	Important	Information Disclosure	4034664 4034733	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows	4038792 (Monthly Rollup) 4036586 (IE	Important	Information Disclosure	4034681 4034733	Base: 4.30 Temporal: 3.90 Vector:	Yes

CVE-2017-8736						
8.1 for 32-bit systems	Cumulative)				CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	
Internet Explorer 11 on Windows 8.1 for x64-based systems	4038792 (Monthly Rollup) 4036586 (IE Cumulative)	Important	Information Disclosure	4034681 4034733	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows RT 8.1	4038792 (Monthly Rollup)	Important	Information Disclosure	4034681	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2008 R2 for x64-	4038777 (Monthly Rollup) 4036586 (IE Cumulative)	Low	Information Disclosure	4034664 4034733	Base: 2.40 Temporal: 2.20 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8736						
based Systems Service Pack 1						
Internet Explorer 11 on Windows Server 2012 R2	4038792 (Monthly Rollup) 4036586 (IE Cumulative)	Low	Information Disclosure	4034681 4034733	Base: 2.40 Temporal: 2.20 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2016	4038782 (Security Update)	Low	Information Disclosure	4034658	Base: 2.40 Temporal: 2.20 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 for 32-bit Systems	4038781 (Security Update)	Important	Information Disclosure	4034668	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8736						
Microsoft Edge on Windows 10 for x64-based Systems	4038781 (Security Update)	Important	Information Disclosure	4034668	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems	4038783 (Security Update)	Important	Information Disclosure	4034660	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version	4038783 (Security Update)	Important	Information Disclosure	4034660	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8736						
1511 for x64-based Systems						
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4038782 (Security Update)	Important	Information Disclosure	4034658	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8736						
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4038788 (Security Update)	Important	Information Disclosure	4034674	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4038788 (Security Update)	Important	Information Disclosure	4034674	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows	4038782 (Security Update)	Low	Information Disclosure	4034658	Base: 2.40 Temporal: 2.20 Vector:	Yes

CVE-2017-8736						
Server 2016					CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	

CVE-2017-8738 - Scripting Engine Memory Corruption Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8738 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 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 update addresses the vulnerability by modifying how the scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8738						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4038781 (Security Update)	Critical	Remote Code Execution	4034668	Base: 4.20 Temporal: 3.80 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	4038781 (Security Update)	Critical	Remote Code Execution	4034668	Base: 4.20 Temporal: 3.80 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 1511 for	4038783 (Security Update)	Critical	Remote Code Execution	4034660	Base: 4.20 Temporal: 3.80 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-2017-8738						
32-bit Systems						
Microsoft Edge on Windows 10 Version 1511 for x64-based Systems	4038783 (Security Update)	Critical	Remote Code Execution	4034660	Base: 4.20 Temporal: 3.80 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	4038782 (Security Update)	Critical	Remote Code Execution	4034658	Base: 4.20 Temporal: 3.80 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	4038782 (Security Update)	Critical	Remote Code Execution	4034658	Base: 4.20 Temporal: 3.80 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-2017-8738						
Microsoft Edge on Windows Server 2016	4038782 (Security Update)	Moderate	Remote Code Execution	4034658	Base: 3.10 Temporal: 2.80 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8739 - Scripting Engine Information Disclosure Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8739 MITRE NVD	**CVE Title:** Scripting Engine Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the scripting engine does not properly handle objects in memory in Microsoft Edge. An attacker who successfully exploited the vulnerability could obtain information to further compromise the user's system. In a web-based attack scenario, an attacker could host a website in an attempt to exploit the vulnerability. In addition, compromised websites and websites that accept or host	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	user-provided content could contain 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. For example, an attacker could trick a user into clicking a link that takes the user to the attacker's site. The security update addresses the vulnerability by changing how the scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8739						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4038788 (Security Update)	Important	Information Disclosure	4034674	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4038788 (Security Update)	Important	Information Disclosure	4034674	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8740 - Scripting Engine Memory Corruption Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8740 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 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 update addresses the vulnerability by modifying how the scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8740						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2017-8740						
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4038788 (Security Update)	Critical	Remote Code Execution	4034674	Base: 4.20 Temporal: 3.80 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	4038788 (Security Update)	Critical	Remote Code Execution	4034674	Base: 4.20 Temporal: 3.80 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-2017-8741 - Scripting Engine Memory Corruption Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8741 MITRE NVD	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that Microsoft browser JavaScript engines render content when handling 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. In a web-based attack scenario, 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. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the related 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. 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. The security update addresses the vulnerability by modifying how Microsoft browser JavaScript scripting engines handle objects in memory.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8741						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2017-8741						
Internet Explorer 10 on Windows Server 2012	4038799 (Monthly Rollup) 4036586 (IE Cumulative)	Moderate	Remote Code Execution	4034665 4034733	Base: 3.10 Temporal: 2.80 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 for 32-bit Systems	4038781 (Security Update)	Critical	Remote Code Execution	4034668	Base: 4.20 Temporal: 3.80 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
Internet Explorer 11 on Windows 10 for x64-based Systems	4038781 (Security Update)	Critical	Remote Code Execution	4034668	Base: 4.20 Temporal: 3.80 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-2017-8741						
Internet Explorer 11 on Windows 10 Version 1511 for 32-bit Systems	4038783 (Security Update)	Critical	Remote Code Execution	4034660	Base: 4.20 Temporal: 3.80 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
Internet Explorer 11 on Windows 10 Version 1511 for x64-based Systems	4038783 (Security Update)	Critical	Remote Code Execution	4034660	Base: 4.20 Temporal: 3.80 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
Internet Explorer 11 on Windows	4038782 (Security Update)	Critical	Remote Code Execution	4034658	Base: 4.20 Temporal: 3.80 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-2017-8741						
10 Version 1607 for 32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4038782 (Security Update)	Critical	Remote Code Execution	4034658	Base: 4.20 Temporal: 3.80 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
Internet Explorer 11 on Windows 10 Version 1703 for	4038788 (Security Update)	Critical	Remote Code Execution	4034674	Base: 4.20 Temporal: 3.80 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-2017-8741						
32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems	4038788 (Security Update)	Critical	Remote Code Execution	4034674	Base: 4.20 Temporal: 3.80 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
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1	4038777 (Monthly Rollup) 4036586 (IE Cumulative)	Critical	Remote Code Execution	4034664 4034733	Base: 4.20 Temporal: 3.80 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-2017-8741						
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1	4038777 (Monthly Rollup) 4036586 (IE Cumulative)	Critical	Remote Code Execution	4034664 4034733	Base: 4.20 Temporal: 3.80 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
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4038792 (Monthly Rollup) 4036586 (IE Cumulative)	Critical	Remote Code Execution	4034681 4034733	Base: 4.20 Temporal: 3.80 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
Internet Explorer 11 on Windows 8.1 for x64-	4038792 (Monthly Rollup) 4036586 (IE Cumulative)	Critical	Remote Code Execution	4034681 4034733	Base: 4.20 Temporal: 3.80 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-2017-8741						
based systems						
Internet Explorer 11 on Windows RT 8.1	4038792 (Monthly Rollup)	Critical	Remote Code Execution	4034681	Base: 4.20 Temporal: 3.80 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
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4038777 (Monthly Rollup) 4036586 (IE Cumulative)	Moderate	Remote Code Execution	4034664 4034733	Base: 3.10 Temporal: 2.80 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows	4038792 (Monthly Rollup) 4036586 (IE Cumulative)	Moderate	Remote Code Execution	4034681 4034733	Base: 3.10 Temporal: 2.80 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8741						
Server 2012 R2						
Internet Explorer 11 on Windows Server 2016	4038782 (Security Update)	Moderate	Remote Code Execution	4034658	Base: 3.10 Temporal: 2.80 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2	4036586 (IE Cumulative)	Moderate	Remote Code Execution	4034733	Base: 3.10 Temporal: 2.80 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 9 on Windows Server	4036586 (IE Cumulative)	Moderate	Remote Code Execution	4034733	Base: 3.10 Temporal: 2.80 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8741						
2008 for x64-based Systems Service Pack 2						
Microsoft Edge on Windows 10 for 32-bit Systems	4038781 (Security Update)	Critical	Remote Code Execution	4034668	Base: 4.20 Temporal: 3.80 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	4038781 (Security Update)	Critical	Remote Code Execution	4034668	Base: 4.20 Temporal: 3.80 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	4038783 (Security Update)	Critical	Remote Code Execution	4034660	Base: 4.20 Temporal: 3.80 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-2017-8741						
Version 1511 for 32-bit Systems						
Microsoft Edge on Windows 10 Version 1511 for x64-based Systems	4038783 (Security Update)	Critical	Remote Code Execution	4034660	Base: 4.20 Temporal: 3.80 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	4038782 (Security Update)	Critical	Remote Code Execution	4034658	Base: 4.20 Temporal: 3.80 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-2017-8741						
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4038782 (Security Update)	Critical	Remote Code Execution	4034658	Base: 4.20 Temporal: 3.80 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	4038788 (Security Update)	Critical	Remote Code Execution	4034674	Base: 4.20 Temporal: 3.80 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	4038788 (Security Update)	Critical	Remote Code Execution	4034674	Base: 4.20 Temporal: 3.80 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-2017-8741						
x64-based Systems						
Microsoft Edge on Windows Server 2016	4038782 (Security Update)	Moderate	Remote Code Execution	4034658	Base: 3.10 Temporal: 2.80 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8742 - PowerPoint Remote Code Execution Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8742 MITRE NVD	**CVE Title:** PowerPoint Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in Microsoft Office 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 Office software. 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) that contains 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. Note that the Preview Pane is not an attack vector for this vulnerability. The security update addresses the vulnerability by correcting how Office handles objects in memory. **FAQ:** None **Mitigations:** None		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Workarounds: None **Revision:** 1.0 2017-09-12T07:00:00 Information Published.		

Affected Software

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

CVE-2017-8742						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Office Compatibility Pack Service Pack 3	3213644 (Security Update)	Important	Remote Code Execution	None	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office Web Apps 2010 Service Pack 2	3213632 (Security Update)	Important	Remote Code Execution	3203466	Base: N/A Temporal:	Maybe

CVE-2017-8742						
					N/A Vector: N/A	
Microsoft Office Web Apps Server 2013 Service Pack 1	3213562 (Security Update)	Important	Remote Code Execution	None	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft PowerPoint 2007 Service Pack 3	3213642 (Security Update)	Important	Remote Code Execution	None	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft PowerPoint 2010 Service Pack 2 (32-bit editions)	3128027 (Security Update)	Important	Remote Code Execution	3118378	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft PowerPoint 2010 Service Pack 2 (64-bit editions)	3128027 (Security Update)	Important	Remote Code Execution	3118378	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft PowerPoint 2013 RT Service Pack 1	4011069 (Security Update)	Important	Remote Code Execution	3115487	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-8742						
Microsoft PowerPoint 2013 Service Pack 1 (32-bit editions)	4011069 (IE Cumulative)	Important	Remote Code Execution	3115487	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft PowerPoint 2013 Service Pack 1 (64-bit editions)	4011069 (IE Cumulative)	Important	Remote Code Execution	3115487	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft PowerPoint 2016 (32-bit edition)	4011041 (Security Update)	Important	Remote Code Execution	3114518	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft PowerPoint 2016 (64-bit edition)	4011041 (Security Update)	Important	Remote Code Execution	3114518	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft PowerPoint Viewer 2007	3128030 (Security Update)	Important	Remote Code Execution	3118382	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Enterprise Server 2016	4011127 (Security Update)	Important	Remote Code Execution	3213544	Base: N/A Temporal:	Unknown

CVE-2017-8742						
					N/A Vector: N/A	
Microsoft SharePoint Server 2013 Service Pack 1	3213560 (Security Update)	Important	Remote Code Execution	None	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-8743 - PowerPoint Remote Code Execution Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8743 MITRE NVD	**CVE Title:** PowerPoint Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in Microsoft Office 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 Office software. 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) that contains 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. Note that the Preview Pane is not an attack vector for this vulnerability. The security update addresses the vulnerability by correcting how Office handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 2017-09-12T07:00:00 Information Published.		

Affected Software

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

CVE-2017-8743						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft PowerPoint 2016 (32-bit edition)	4011041 (Security Update)	Important	Remote Code Execution	3114518	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft PowerPoint 2016 (64-bit edition)	4011041 (Security Update)	Important	Remote Code Execution	3114518	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-8743						
Microsoft SharePoint Enterprise Server 2016	4011127 (Security Update)	Important	Remote Code Execution	3213544	Base: N/A Temporal: N/A Vector: N/A	Unknown
Office Online Server	3213658 (Security Update)	Important	Remote Code Execution	None	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-8725 - Microsoft Office Publisher Remote Code Execution

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8725 MITRE NVD	**CVE Title:** Microsoft Office Publisher Remote Code Execution **Description:** A remote code execution vulnerability exists in Microsoft Office software when it fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could use a specially crafted file to perform actions in the security context	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	of the current user. For example, the file could then take actions on behalf of the logged-on user with the same permissions as the current user. Exploitation of this vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Office software. 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) that contains a specially crafted file that is designed to exploit the vulnerability. However, an attacker would have no way to force the user to visit the website. Instead, an attacker would have to convince the user to click a link, typically by way of an enticement in an email or Instant Messenger message, and then convince the user to open the specially crafted file. The security update addresses the vulnerability by correcting how Microsoft Office handles files in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 2017-09-12T07:00:00 Information Published.		

Affected Software

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

CVE-2017-8725						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Publisher 2007 Service Pack 3	3114428 (Security Update)	Important	Remote Code Execution	None	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Publisher 2010 Service Pack 2 (32-bit editions)	3141537 (Security Update)	Important	Remote Code Execution	3114395	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-8725						
Microsoft Publisher 2010 Service Pack 2 (64-bit editions)	3141537 (Security Update)	Important	Remote Code Execution	3114395	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-8735 - Microsoft Edge Spoofing Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8735 MITRE NVD	**CVE Title:** Microsoft Edge Spoofing Vulnerability **Description:** A spoofing vulnerability exists when Microsoft Edge does not properly parse HTTP content. An attacker who successfully exploited this vulnerability could trick a user by redirecting the user to a specially crafted website. The specially crafted website could either spoof content or serve as a pivot to chain an attack with other vulnerabilities in web services.	Low	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	To exploit the vulnerability, the user must click a specially crafted URL. In an email attack scenario, an attacker could send an email message containing the specially crafted URL to the user in an attempt to convince the user to click it. In a web-based attack scenario, an attacker could host a specially crafted website designed to appear as a legitimate website to the user. However, the attacker would have no way to force the user to visit the specially crafted website. The attacker would have to convince the user to visit the specially crafted website, typically by way of enticement in an email or instant message, and then convince the user to interact with content on the website. The update addresses the vulnerability by correcting how Microsoft Edge parses HTTP responses. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8735						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4038781 (Security Update)	Moderate	Spoofing	4034668	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 for x64-based Systems	4038781 (Security Update)	Moderate	Spoofing	4034668	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1511 for	4038783 (Security Update)	Moderate	Spoofing	4034660	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8735						
32-bit Systems						
Microsoft Edge on Windows 10 Version 1511 for x64-based Systems	4038783 (Security Update)	Moderate	Spoofing	4034660	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4038782 (Security Update)	Moderate	Spoofing	4034658	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4038782 (Security Update)	Moderate	Spoofing	4034658	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8735						
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4038788 (Security Update)	Moderate	Spoofing	4034674	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4038788 (Security Update)	Moderate	Spoofing	4034674	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server 2016	4038782 (Security Update)	Low	Spoofing	4034658	Base: 2.40 Temporal: 2.20 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8746 - Device Guard Security Feature Bypass Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8746 MITRE NVD	**CVE Title:** Device Guard Security Feature Bypass Vulnerability **Description:** A security feature bypass vulnerability exists in Device Guard that could allow an attacker to inject malicious code into a Windows PowerShell session. An attacker who successfully exploited this vulnerability could inject code into a trusted PowerShell process to bypass the Device Guard Code Integrity policy on the local machine. To exploit the vulnerability, an attacker would first have to access the local machine, and then inject malicious code into a script that is trusted by the Code Integrity policy. The injected code would then run with the same trust level as the script and bypass the Code Integrity policy. The update addresses the vulnerability by correcting how PowerShell exposes functions and processes user supplied code. **FAQ:** None **Mitigations:** None	Important	Security Feature Bypass

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Workarounds: None **Revision:** 1.0 2017-09-12T07:00:00 Information Published.		

Affected Software

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

CVE-2017-8746						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1607 for 32-bit Systems	4038782 (Security Update)	Important	Security Feature Bypass	4034658	Base: 5.30 Temporal: 4.80 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-	4038782 (Security Update)	Important	Security Feature Bypass	4034658	Base: 5.30 Temporal: 4.80	Yes

CVE-2017-8746						
based Systems					Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	
Windows 10 Version 1703 for 32-bit Systems	4038788 (Security Update)	Important	Security Feature Bypass	4034674	Base: 5.30 Temporal: 4.80 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4038788 (Security Update)	Important	Security Feature Bypass	4034674	Base: 5.30 Temporal: 4.80 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2016	4038782 (Security Update)	Important	Security Feature Bypass	4034658	Base: 5.30 Temporal: 4.80 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4038782 (Security Update)	Important	Security Feature Bypass	4034658	Base: 5.30 Temporal: 4.80 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2017-8747 - Internet Explorer Memory Corruption Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8747 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. 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. 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 Internet Explorer handles objects in memory. **FAQ:** None **Mitigations:**	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8747						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 10 on Windows Server 2012	4038799 (Monthly Rollup) 4036586 (IE Cumulative)	Moderate	Remote Code Execution	4034665 4034733	Base: 6.40 Temporal: 5.80 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-2017-8747						
Internet Explorer 11 on Windows 10 for 32-bit Systems	4038781 (Security Update)	Critical	Remote Code Execution	4034668	Base: 7.50 Temporal: 6.70 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	4038781 (Security Update)	Critical	Remote Code Execution	4034668	Base: 7.50 Temporal: 6.70 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 1511 for	4038783 (Security Update)	Critical	Remote Code Execution	4034660	Base: 7.50 Temporal: 6.70 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-2017-8747						
32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1511 for x64-based Systems	4038783 (Security Update)	Critical	Remote Code Execution	4034660	Base: 7.50 Temporal: 6.70 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 32-bit Systems	4038782 (Security Update)	Critical	Remote Code Execution	4034658	Base: 7.50 Temporal: 6.70 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-2017-8747						
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4038782 (Security Update)	Critical	Remote Code Execution	4034658	Base: 7.50 Temporal: 6.70 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	4038788 (Security Update)	Critical	Remote Code Execution	4034674	Base: 7.50 Temporal: 6.70 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	4038788 (Security Update)	Critical	Remote Code Execution	4034674	Base: 7.50 Temporal: 6.70 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-2017-8747						
10 Version 1703 for x64-based Systems						
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1	4038777 (Monthly Rollup) 4036586 (IE Cumulative)	Critical	Remote Code Execution	4034664 4034733	Base: 7.50 Temporal: 6.70 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	4038777 (Monthly Rollup) 4036586 (IE Cumulative)	Critical	Remote Code Execution	4034664 4034733	Base: 7.50 Temporal: 6.70 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-2017-8747						
Service Pack 1						
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4038792 (Monthly Rollup) 4036586 (IE Cumulative)	Critical	Remote Code Execution	4034681 4034733	Base: 7.50 Temporal: 6.70 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	4038792 (Monthly Rollup) 4036586 (IE Cumulative)	Critical	Remote Code Execution	4034681 4034733	Base: 7.50 Temporal: 6.70 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 RT 8.1	4038792 (Monthly Rollup)	Critical	Remote Code Execution	4034681	Base: 7.50 Temporal: 6.70 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-2017-8747						
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4038777 (Monthly Rollup) 4036586 (IE Cumulative)	Moderate	Remote Code Execution	4034664 4034733	Base: 6.40 Temporal: 5.80 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 R2	4038792 (Monthly Rollup) 4036586 (IE Cumulative)	Moderate	Remote Code Execution	4034681 4034733	Base: 6.40 Temporal: 5.80 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 2016	4038782 (Security Update)	Moderate	Remote Code Execution	4034658	Base: 6.40 Temporal: 5.80 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-2017-8749 - Internet Explorer Memory Corruption Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8749 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. 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. 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 Internet Explorer handles objects in memory. **FAQ:** None **Mitigations:**	Moderate	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8749						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 10 on Windows Server 2012	4038799 (Monthly Rollup) 4036586 (IE Cumulative)	Moderate	Remote Code Execution	4034665 4034733	Base: 6.40 Temporal: 5.80 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-2017-8749						
Internet Explorer 11 on Windows 10 for 32-bit Systems	4038781 (Security Update)	Critical	Remote Code Execution	4034668	Base: 7.50 Temporal: 6.70 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	4038781 (Security Update)	Critical	Remote Code Execution	4034668	Base: 7.50 Temporal: 6.70 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 1511 for	4038783 (Security Update)	Critical	Remote Code Execution	4034660	Base: 7.50 Temporal: 6.70 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-2017-8749						
32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1511 for x64-based Systems	4038783 (Security Update)	Critical	Remote Code Execution	4034660	Base: 7.50 Temporal: 6.70 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 32-bit Systems	4038782 (Security Update)	Critical	Remote Code Execution	4034658	Base: 7.50 Temporal: 6.70 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-2017-8749						
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4038782 (Security Update)	Critical	Remote Code Execution	4034658	Base: 7.50 Temporal: 6.70 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	4038788 (Security Update)	Critical	Remote Code Execution	4034674	Base: 7.50 Temporal: 6.70 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	4038788 (Security Update)	Critical	Remote Code Execution	4034674	Base: 7.50 Temporal: 6.70 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-2017-8749						
10 Version 1703 for x64-based Systems						
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1	4038777 (Monthly Rollup) 4036586 (IE Cumulative)	Critical	Remote Code Execution	4034664 4034733	Base: 7.50 Temporal: 6.70 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	4038777 (Monthly Rollup) 4036586 (IE Cumulative)	Critical	Remote Code Execution	4034664 4034733	Base: 7.50 Temporal: 6.70 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-2017-8749						
Service Pack 1						
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4038792 (Monthly Rollup) 4036586 (IE Cumulative)	Critical	Remote Code Execution	4034681 4034733	Base: 7.50 Temporal: 6.70 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	4038792 (Monthly Rollup) 4036586 (IE Cumulative)	Critical	Remote Code Execution	4034681 4034733	Base: 7.50 Temporal: 6.70 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 RT 8.1	4038792 (Monthly Rollup)	Critical	Remote Code Execution	4034681	Base: 7.50 Temporal: 6.70 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-2017-8749						
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4038777 (Monthly Rollup) 4036586 (IE Cumulative)	Moderate	Remote Code Execution	4034664 4034733	Base: 6.40 Temporal: 5.80 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 R2	4038792 (Monthly Rollup) 4036586 (IE Cumulative)	Moderate	Remote Code Execution	4034681 4034733	Base: 6.40 Temporal: 5.80 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 2016	4038782 (Security Update)	Moderate	Remote Code Execution	4034658	Base: 6.40 Temporal: 5.80 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-2017-8750 - Microsoft Browser Memory Corruption Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8750 MITRE NVD	**CVE Title:** Microsoft Browser Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists when Microsoft browsers improperly access 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. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through a Microsoft browser, 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 Microsoft browsers handle objects in memory. **FAQ:**	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information published. 1.1 2017-09-12T07:00:00 Updated acknowledgment. This is an informational change only.		

Affected Software

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

CVE-2017-8750						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2017-8750						
Internet Explorer 11 on Windows 10 for 32-bit Systems	4038781 (Security Update)	Critical	Remote Code Execution	4034668	Base: 7.50 Temporal: 6.70 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	4038781 (Security Update)	Critical	Remote Code Execution	4034668	Base: 7.50 Temporal: 6.70 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 1511 for	4038783 (Security Update)	Critical	Remote Code Execution	4034660	Base: 7.50 Temporal: 6.70 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-2017-8750						
32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1511 for x64-based Systems	4038783 (Security Update)	Critical	Remote Code Execution	4034660	Base: 7.50 Temporal: 6.70 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 32-bit Systems	4038782 (Security Update)	Critical	Remote Code Execution	4034658	Base: 7.50 Temporal: 6.70 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-2017-8750						
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4038782 (Security Update)	Critical	Remote Code Execution	4034658	Base: 7.50 Temporal: 6.70 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	4038788 (Security Update)	Critical	Remote Code Execution	4034674	Base: 7.50 Temporal: 6.70 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	4038788 (Security Update)	Critical	Remote Code Execution	4034674	Base: 7.50 Temporal: 6.70 Vector:	Yes

CVE-2017-8750						
10 Version 1703 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 7 for 32-bit Systems Service Pack 1	4038777 (Monthly Rollup) 4036586 (IE Cumulative)	Critical	Remote Code Execution	4034664 4034733	Base: 7.50 Temporal: 6.70 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	4038777 (Monthly Rollup) 4036586 (IE Cumulative)	Critical	Remote Code Execution	4034664 4034733	Base: 7.50 Temporal: 6.70 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-2017-8750						
Service Pack 1						
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4038792 (Monthly Rollup) 4036586 (IE Cumulative)	Critical	Remote Code Execution	4034681 4034733	Base: 7.50 Temporal: 6.70 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	4038792 (Monthly Rollup) 4036586 (IE Cumulative)	Critical	Remote Code Execution	4034681 4034733	Base: 7.50 Temporal: 6.70 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 RT 8.1	4038792 (Monthly Rollup)	Critical	Remote Code Execution	4034681	Base: 7.50 Temporal: 6.70 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-2017-8750						
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4038777 (Monthly Rollup) 4036586 (IE Cumulative)	Moderate	Remote Code Execution	4034664 4034733	Base: 6.40 Temporal: 5.80 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 R2	4038792 (Monthly Rollup) 4036586 (IE Cumulative)	Moderate	Remote Code Execution	4034681 4034733	Base: 6.40 Temporal: 5.80 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 2016	4038782 (Security Update)	Moderate	Remote Code Execution	4034658	Base: 6.40 Temporal: 5.80 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-2017-8750						
Microsoft Edge on Windows 10 for 32-bit Systems	4038781 (Security Update)	Critical	Remote Code Execution	4034668	Base: 4.20 Temporal: 3.80 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	4038781 (Security Update)	Critical	Remote Code Execution	4034668	Base: 4.20 Temporal: 3.80 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 1511 for	4038783 (Security Update)	Critical	Remote Code Execution	4034660	Base: 4.20 Temporal: 3.80 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-2017-8750						
32-bit Systems						
Microsoft Edge on Windows 10 Version 1511 for x64-based Systems	4038783 (Security Update)	Critical	Remote Code Execution	4034660	Base: 4.20 Temporal: 3.80 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	4038782 (Security Update)	Critical	Remote Code Execution	4034658	Base: 4.20 Temporal: 3.80 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-2017-8750						
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4038782 (Security Update)	Critical	Remote Code Execution	4034658	Base: 4.20 Temporal: 3.80 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	4038782 (Security Update)	Moderate	Remote Code Execution	4034658	Base: 4.20 Temporal: 3.80 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-2017-8751 - Microsoft Edge Memory Corruption Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8751 MITRE NVD	**CVE Title:** Microsoft Edge Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory. The vulnerability could corrupt memory in such a way that enables 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, an 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 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 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 by way of enticement in an email or Instant Messenger message, or by getting them to open an attachment sent through email. The security update addresses the vulnerability by modifying how Microsoft Edge handles objects in memory. **FAQ:**	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information Published.		

Affected Software

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

CVE-2017-8751						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version	4038788 (Security Update)	Critical	Remote Code Execution	4034674	Base: 4.20 Temporal: 3.80 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-2017-8751						
1703 for 32-bit Systems						
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4038788 (Security Update)	Critical	Remote Code Execution	4034674	Base: 4.20 Temporal: 3.80 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-2017-8752 - Scripting Engine Memory Corruption Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8752	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:**	Critical	Remote Code Execution

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8752						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems	4038783 (Security Update)	Critical	Remote Code Execution	4034660	Base: 4.20 Temporal: 3.80 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-2017-8752						
Microsoft Edge on Windows 10 Version 1511 for x64-based Systems	4038783 (Security Update)	Critical	Remote Code Execution	4034660	Base: 4.20 Temporal: 3.80 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	4038782 (Security Update)	Critical	Remote Code Execution	4034658	Base: 4.20 Temporal: 3.80 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	4038782 (Security Update)	Critical	Remote Code Execution	4034658	Base: 4.20 Temporal: 3.80 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-2017-8752						
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4038788 (Security Update)	Critical	Remote Code Execution	4034674	Base: 4.20 Temporal: 3.80 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	4038788 (Security Update)	Critical	Remote Code Execution	4034674	Base: 4.20 Temporal: 3.80 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	4038782 (Security Update)	Moderate	Remote Code Execution	4034658	Base: 4.20 Temporal: 3.80 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-2017-8753 - Scripting Engine Memory Corruption Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8753 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 Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability. The update addresses the vulnerability by modifying how the scripting engine handles objects in memory. **FAQ:** None **Mitigations:**	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8753						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4038781 (Security Update)	Critical	Remote Code Execution	4034668	Base: 4.20 Temporal: 3.80 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-2017-8753						
Microsoft Edge on Windows 10 for x64-based Systems	4038781 (Security Update)	Critical	Remote Code Execution	4034668	Base: 4.20 Temporal: 3.80 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 1511 for 32-bit Systems	4038783 (Security Update)	Critical	Remote Code Execution	4034660	Base: 4.20 Temporal: 3.80 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 1511 for x64-based Systems	4038783 (Security Update)	Critical	Remote Code Execution	4034660	Base: 4.20 Temporal: 3.80 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	4038782 (Security Update)	Critical	Remote Code Execution	4034658	Base: 4.20 Temporal: 3.80	Yes

CVE-2017-8753						
10 Version 1607 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 1607 for x64-based Systems	4038782 (Security Update)	Critical	Remote Code Execution	4034658	Base: 4.20 Temporal: 3.80 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	4038788 (Security Update)	Critical	Remote Code Execution	4034674	Base: 4.20 Temporal: 3.80 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	4038788 (Security Update)	Critical	Remote Code Execution	4034674	Base: 4.20 Temporal: 3.80 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-2017-8753						
x64-based Systems						
Microsoft Edge on Windows Server 2016	4038782 (Security Update)	Moderate	Remote Code Execution	4034658	Base: 4.20 Temporal: 3.80 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-2017-8754 - Microsoft Edge Security Feature Bypass Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8754 MITRE NVD	**CVE Title:** Microsoft Edge Security Feature Bypass Vulnerability **Description:** A security feature bypass exists in Microsoft Edge when the Edge Content Security Policy (CSP) fails to properly validate certain specially crafted documents. An attacker who exploited the bypass could trick a user into loading a page containing malicious content.	Low	Security Feature Bypass

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	To exploit the bypass, an attacker must trick a user into either loading a page containing malicious content or visiting a malicious website. The attacker could also inject the malicious page into either a compromised website or an advertisement network. The update addresses the bypass by correcting how the Edge CSP validates documents. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8754						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4038781 (Security Update)	Important	Security Feature Bypass	4034668	Base: 4.20 Temporal: 3.80 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	4038781 (Security Update)	Important	Security Feature Bypass	4034668	Base: 4.20 Temporal: 3.80 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 1511 for 32-bit Systems	4038783 (Security Update)	Important	Security Feature Bypass	4034660	Base: 4.20 Temporal: 3.80 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	4038783 (Security Update)	Important	Security Feature Bypass	4034660	Base: 4.20 Temporal: 3.80	Yes

CVE-2017-8754						
10 Version 1511 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 1607 for 32-bit Systems	4038782 (Security Update)	Important	Security Feature Bypass	4034658	Base: 4.20 Temporal: 3.80 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	4038782 (Security Update)	Important	Security Feature Bypass	4034658	Base: 4.20 Temporal: 3.80 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	4038788 (Security Update)	Important	Security Feature Bypass	4034674	Base: 4.20 Temporal: 3.80 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-2017-8754						
32-bit Systems						
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4038788 (Security Update)	Important	Security Feature Bypass	4034674	Base: 4.20 Temporal: 3.80 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	4038782 (Security Update)	Low	Security Feature Bypass	4034658	Base: 4.20 Temporal: 3.80 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-2017-8755 - Scripting Engine Memory Corruption Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8755 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 Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability. The update addresses the vulnerability by modifying how the scripting engine handles objects in memory. **FAQ:** None **Mitigations:**	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information Published.		

Affected Software

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

CVE-2017-8755						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1511 for	4038783 (Security Update)	Critical	Remote Code Execution	4034660	Base: 4.20 Temporal: 3.80 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-2017-8755						
32-bit Systems						
Microsoft Edge on Windows 10 Version 1511 for x64-based Systems	4038783 (Security Update)	Critical	Remote Code Execution	4034660	Base: 4.20 Temporal: 3.80 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	4038782 (Security Update)	Critical	Remote Code Execution	4034658	Base: 4.20 Temporal: 3.80 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	4038782 (Security Update)	Critical	Remote Code Execution	4034658	Base: 4.20 Temporal: 3.80 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-2017-8755						
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4038788 (Security Update)	Critical	Remote Code Execution	4034674	Base: 4.20 Temporal: 3.80 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	4038788 (Security Update)	Critical	Remote Code Execution	4034674	Base: 4.20 Temporal: 3.80 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	4038782 (Security Update)	Moderate	Remote Code Execution	4034658	Base: 4.20 Temporal: 3.80 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-2017-8756 - Scripting Engine Memory Corruption Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8756 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 Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability. The update addresses the vulnerability by modifying how the scripting engine handles objects in memory.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8756						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2017-8756						
Microsoft Edge on Windows 10 for 32-bit Systems	4038781 (Security Update)	Critical	Remote Code Execution	4034668	Base: 4.20 Temporal: 3.80 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	4038781 (Security Update)	Critical	Remote Code Execution	4034668	Base: 4.20 Temporal: 3.80 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 1511 for 32-bit Systems	4038783 (Security Update)	Critical	Remote Code Execution	4034660	Base: 4.20 Temporal: 3.80 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	4038783 (Security Update)	Critical	Remote Code Execution	4034660	Base: 4.20 Temporal: 3.80 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-2017-8756						
1511 for x64-based Systems						
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4038782 (Security Update)	Critical	Remote Code Execution	4034658	Base: 4.20 Temporal: 3.80 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	4038782 (Security Update)	Critical	Remote Code Execution	4034658	Base: 4.20 Temporal: 3.80 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	4038788 (Security Update)	Critical	Remote Code Execution	4034674	Base: 4.20 Temporal: 3.80 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-2017-8756						
32-bit Systems						
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4038788 (Security Update)	Critical	Remote Code Execution	4034674	Base: 4.20 Temporal: 3.80 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	4038782 (Security Update)	Moderate	Remote Code Execution	4034658	Base: 4.20 Temporal: 3.80 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-2017-8757 - Microsoft Edge Remote Code Execution Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8757 MITRE NVD	**CVE Title:** Microsoft Edge Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in the way Microsoft Edge handles objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge and then convince a user to view the website. In addition, an attacker could embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the browser rendering engine. Finally, the attacker could 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 Microsoft Edge handles objects in memory. **FAQ:**	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-8757						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-	4038781 (Security Update)	Critical	Remote Code Execution	4034668	Base: 4.20 Temporal: 3.80 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-2017-8757						
bit Systems						
Microsoft Edge on Windows 10 for x64-based Systems	4038781 (Security Update)	Critical	Remote Code Execution	4034668	Base: 4.20 Temporal: 3.80 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 1511 for 32-bit Systems	4038783 (Security Update)	Critical	Remote Code Execution	4034660	Base: 4.20 Temporal: 3.80 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 1511 for x64-based Systems	4038783 (Security Update)	Critical	Remote Code Execution	4034660	Base: 4.20 Temporal: 3.80 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-2017-8757						
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4038782 (Security Update)	Critical	Remote Code Execution	4034658	Base: 4.20 Temporal: 3.80 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	4038782 (Security Update)	Critical	Remote Code Execution	4034658	Base: 4.20 Temporal: 3.80 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	4038788 (Security Update)	Critical	Remote Code Execution	4034674	Base: 4.20 Temporal: 3.80 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-2017-8757						
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4038788 (Security Update)	Critical	Remote Code Execution	4034674	Base: 4.20 Temporal: 3.80 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	4038782 (Security Update)	Moderate	Remote Code Execution	4034658	Base: 4.20 Temporal: 3.80 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-2017-11761 - Microsoft Exchange Information Disclosure Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11761 MITRE NVD	**CVE Title:** Microsoft Exchange Information Disclosure Vulnerability **Description:** An input sanitization issue exists with Microsoft Exchange that could potentially result in unintended Information Disclosure. An attacker who successfully exploited the vulnerability could identify the existence of RFC1918 addresses on the local network from a client on the Internet. An attacker could use this internal host information as part of a larger attack. To exploit the vulnerability, an attacker could include specially crafted tags in Calendar-related messages sent to an Exchange server. These specially-tagged messages could prompt the Exchange server to fetch information from internal servers. By observing telemetry from these requests, a client could discern properties of internal hosts intended to be hidden from the Internet. The update corrects the way that Exchange parses Calendar-related messages. **FAQ:** None **Mitigations:** None **Workarounds:** None	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-11761						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Exchange Server 2013 Cumulative Update 16	4036108 (Security Update)	Important	Information Disclosure	4018588	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Exchange Server 2013 Cumulative Update 17	4036108 (Security Update)	Important	Information Disclosure	None	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2017-11761						
Microsoft Exchange Server 2013 Service Pack 1	4036108 (Security Update)	Important	Information Disclosure	4018588	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Exchange Server 2016 Cumulative Update 5	4036108 (Security Update)	Important	Information Disclosure	4018588	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Exchange Server 2016 Cumulative Update 6	4036108 (Security Update)	Important	Information Disclosure	None	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2017-11764 - Scripting Engine Memory Corruption Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11764 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 Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability. The update addresses the vulnerability by modifying how the scripting engine handles objects in memory. **FAQ:** None **Mitigations:**	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-11764						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1607 for	4038782 (Security Update)	Critical	Remote Code Execution	4034658	Base: 4.20 Temporal: 3.80 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-2017-11764						
32-bit Systems						
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4038782 (Security Update)	Critical	Remote Code Execution	4034658	Base: 4.20 Temporal: 3.80 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	4038788 (Security Update)	Critical	Remote Code Execution	4034674	Base: 4.20 Temporal: 3.80 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	4038788 (Security Update)	Critical	Remote Code Execution	4034674	Base: 4.20 Temporal: 3.80 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-2017-11764						
Microsoft Edge on Windows Server 2016	4038782 (Security Update)	Moderate	Remote Code Execution	4034658	Base: 4.20 Temporal: 3.80 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-2017-11766 - Microsoft Edge Memory Corruption Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11766 MITRE NVD	**CVE Title:** Microsoft Edge Memory Corruption Vulnerability **Description:** A vulnerability exists when Microsoft Edge 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. To exploit the vulnerability, an attacker could host a specially crafted website 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-	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 way of enticement in an email or Instant Messenger message, or by opening an attachment sent through email. The update addresses the vulnerability by modifying how Microsoft Edge handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-09-12T07:00:00 Information published.		

Affected Software

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

CVE-2017-11766						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4038781 (Security Update)	Critical	Remote Code Execution	4034668	Base: 4.20 Temporal: 3.80 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	4038781 (Security Update)	Critical	Remote Code Execution	4034668	Base: 4.20 Temporal: 3.80 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 1511 for	4038783 (Security Update)	Critical	Remote Code Execution	4034660	Base: 4.20 Temporal: 3.80 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-2017-11766						
32-bit Systems						
Microsoft Edge on Windows 10 Version 1511 for x64-based Systems	4038783 (Security Update)	Critical	Remote Code Execution	4034660	Base: 4.20 Temporal: 3.80 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	4038782 (Security Update)	Critical	Remote Code Execution	4034658	Base: 4.20 Temporal: 3.80 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	4038782 (Security Update)	Critical	Remote Code Execution	4034658	Base: 4.20 Temporal: 3.80 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-2017-11766						
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4038788 (Security Update)	Critical	Remote Code Execution	4034674	Base: 4.20 Temporal: 3.80 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	4038788 (Security Update)	Critical	Remote Code Execution	4034674	Base: 4.20 Temporal: 3.80 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	4038782 (Security Update)	Moderate	Remote Code Execution	4034658	Base: 4.20 Temporal: 3.80 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-2017-8759 - .NET Framework Remote Code Execution Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8759 MITRE NVD	**CVE Title:** .NET Framework Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when Microsoft .NET Framework processes untrusted input. An attacker who successfully exploited this vulnerability in software using the .NET framework 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. 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. To exploit the vulnerability, an attacker would first need to convince the user to open a malicious document or application. The security update addresses the vulnerability by correcting how .NET validates untrusted input. **FAQ:** **How do I determine which version of Microsoft .NET Framework is installed on my system?** You can install and run multiple versions of .NET Framework on a system, and you can install the versions in any order. For more information, see Microsoft Knowledge Base Article 318785.	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>
How do I locate the updates for the versions of .NET Framework installed on my system?
The download links in the Affected Products table are to the Parent KB number in the Microsoft Update Catalog. To locate the packages you need to download, in the Microsoft Update Catalog, click Download for the platform you have installed on your system. In the Download window, click to download each update that is applicable to your system.
Customers who have updates automatically installed will be offered the Parent KB; however, the package KB numbers listed for each platform will be displayed in Add Remove Programs.
The following table lists the Parent KB numbers for the Monthly Rollup Releases and the Security Only Releases, and the package KB numbers they contain. For more information about Microsoft's update servicing model for Microsoft .NET Framework, see this Microsoft .NET Blog Post.
<table>
<tr><th></th><th colspan="2">Monthly Rollup Release</th><th colspan="2">Security Only Release</th></tr>
<tr><td>Platform</td><td>Parent KB</td><td>Child KBs</td><td>Parent KB</td><td>Child KBs</td></tr>
<tr><td>Windows Server 2008</td><td>4041086</td><td>4040978 - .NET Framework 2.0
4040977 - .NET Framework 4.5.2
4040973 - .NET Framework 4.6</td><td>4041093</td><td>4040964 - .NET Frame
4040960- .NET Frame
4040957 - .NET Frame</td></tr>
<tr><td>Windows 7
Windows Server 2008 R2</td><td>4041083</td><td>4040980 - .NET Framework 3.5.1
4040977 - .NET Framework 4.5.2
4040973 - .NET Framework 4.6/4.6.1/4.6.2/4.7</td><td>4041090</td><td>4040966 - .NET Frame
4040960- .NET Frame
4040957 - .NET Frame
4.6/4.6.1/4.6.2/4.7</td></tr>
</table>
</td><td></td><td></td></tr>
</table>

CVE ID	Vulnerability Description					Maximum Severity Rating	Vulnerability Impact
	Windows Server 2012	4041084	4040979 - .NET Framework 3.5 4040975 - .NET Framework 4.5.2 4040971 - .NET Framework 4.6/4.6.1/4.6.2/4.7	4041091	4040965 - .NET Framework 3.5 4040959 - .NET Framework 4.5.2 4040955 - .NET Framework 4.6/4.6.1/4.6.2/4.7		
	Windows 8.1 Windows Server 2012 R2	4041085	4040981 - .NET Framework 3.5 4040974 - .NET Framework 4.5.2 4040972 - .NET Framework 4.6/4.6.1/4.6.2/4.72	4041092	4040967 - .NET Framework 3.5 4040958 - .NET Framework 4.5.2 4040956 - .NET Framework 4.6/4.6.1/4.6.2/4.7		
	Windows 10 Platforms	**Parent KB**	**.NET Framework Product**				
	Windows 10	4038781	.NET Framework 3.5 .NET Framework 4.6		None		
	Windows 10 Version 1511	4038783	.NET Framework 3.5 .NET Framework 4.6.1		None		
	Windows 10 Version 1607	4038782	.NET Framework 3.5 .NET Framework 4.6.2/4.7		None		
	Windows Server 2016	4038782	.NET Framework 3.5 .NET Framework 4.6.2/4.7		None		

CVE ID	Vulnerability Description					Maximum Severity Rating	Vulnerability Impact
	Windows 10 Version 1703	4038788	.NET Framework 3.5 .NET Framework 4.7		None		
	Mitigations: None **Workarounds:** None **Revision:** 1.1 2017-09-12T07:00:00 Corrected Product versions and supersedence entries in the Affected Products table, corrected .NET versions in the table in the FAQ, and updated the acknowledgment. These are informational changes only. Customers who have already successfully installed the updates do not need to take any further action. 1.0 2017-09-12T07:00:00 Information published.						

Affected Software

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

CVE-2017-8759						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft .NET Framework 2.0 Service Pack 2 on Windows Server 2008 for 32-bit Systems Service Pack 2	4040978 (Monthly Rollup) 4040964 (Security Only)	Important	Remote Code Execution	4019115, 4035039, 4014984, 4032116 2978116	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	4040978 (Monthly Rollup) 4040964 (Security Only)	Important	Remote Code Execution	4019115, 4035039, 4014984, 4032116 2978116	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	4040978 (Monthly Rollup) 4040964 (Security Only)	Important	Remote Code Execution	4019115, 4035039, 4014984, 4032116 2978116	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows 10 for 32-bit Systems	4038781 (Security Update)	Important	Remote Code Execution	4034668	Base: N/A Temporal: N/A	Yes

CVE-2017-8759						
					Vector: N/A	
Microsoft .NET Framework 3.5 on Windows 10 for x64-based Systems	4038781 (Security Update)	Important	Remote Code Execution	4034668	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1511 for 32-bit Systems	4038783 (Security Update)	Important	Remote Code Execution	4034660	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1511 for x64-based Systems	4038783 (Security Update)	Important	Remote Code Execution	4034660	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1607 for 32-bit Systems	4038782 (Security Update)	Important	Remote Code Execution	4034658	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2017-8759						
Microsoft .NET Framework 3.5 on Windows 10 Version 1607 for x64-based Systems	4038782 (Security Update)	Important	Remote Code Execution	4034658	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1703 for 32-bit Systems	4038788 (Security Update)	Important	Remote Code Execution	4034674	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1703 for x64-based Systems	4038788 (Security Update)	Important	Remote Code Execution	4034674	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 8.1 for 32-bit systems	4040981 (Monthly Rollup) 4040967 (Security Only)	Important	Remote Code Execution	4019114, 4035038, 4014983, 4032115 2978122	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-8759						
Microsoft .NET Framework 3.5 on Windows 8.1 for x64-based systems	4040981 (Monthly Rollup) 4040967 (Security Only)	Important	Remote Code Execution	4019114, 4035038, 4014983, 4032115 2978122	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2012	4040979 (Monthly Rollup) 4040965 (Security Only)	Important	Remote Code Execution	4019113, 4035037, 4014982, 4032114 2978121	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2012 (Server Core installation)	4040979 (Monthly Rollup) 4040965 (Security Only)	Important	Remote Code Execution	4019113, 4035037, 4014982, 4032114 2978121	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2012 R2	4040981 (Monthly Rollup) 4040967	Important	Remote Code Execution	4019114, 4035038, 4014983, 4032115 2978122	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-8759						
	(Security Only)					
Microsoft .NET Framework 3.5 on Windows Server 2016	4038782 (Security Update)	Important	Remote Code Execution	4034658	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows Server 2016 (Server Core installation)	4038782 (Security Update)	Important	Remote Code Execution	4034658	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	4040980 (Monthly Rollup) 4040966 (Security Only)	Important	Remote Code Execution	4019112, 4035036, 4014981, 4032113 2978120	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	4040980 (Monthly Rollup) 4040966	Important	Remote Code Execution	4019112, 4035036, 4014981, 4032113 2978120	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-8759						
	(Security Only)					
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4040980 (Monthly Rollup) 4040966 (Security Only)	Important	Remote Code Execution	4019112, 4035036, 4014981, 4032113 2978120	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	4040980 (Monthly Rollup) 4040966 (Security Only)	Important	Remote Code Execution	4019112, 4035036, 4014981, 4032113 2978120	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)	4040980 (Monthly Rollup) 4040966 (Security Only)	Important	Remote Code Execution	4019112, 4035036, 4014981, 4032113 2978120	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	4040977 (Monthly Rollup)	Important	Remote Code Execution	4019115, 4035039, 4014984, 4032116, 4019112, 4035036,	Base: N/A Temporal: N/A	Maybe

CVE-2017-8759						
	4040960 (Security Only)			4014981, 4032113 2978128	Vector: N/A	
Microsoft .NET Framework 4.5.2 on Windows 7 for x64-based Systems Service Pack 1	4040977 (Monthly Rollup) 4040960 (Security Only)	Important	Remote Code Execution	4019115, 4035039, 4014984, 4032116, 4019112, 4035036, 4014981, 4032113 2978128	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows 8.1 for 32-bit systems	4040974 (Monthly Rollup) 4040958 (Security Only)	Important	Remote Code Execution	4019114, 4035038, 4014983, 4032115 2978126	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows 8.1 for x64-based systems	4040974 (Monthly Rollup) 4040958 (Security Only)	Important	Remote Code Execution	4019114, 4035038, 4014983, 4032115 2978126	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-8759						
Microsoft .NET Framework 4.5.2 on Windows RT 8.1	4040974 (Monthly Rollup)	Important	Remote Code Execution	4019114, 4035038, 4014983, 4032115	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	4041086 (Monthly Rollup) 4040960 (Security Only)	Important	Remote Code Execution	4019115, 4035039, 4014984, 4032116, 4019112, 4035036, 4014981, 4032113 2978128	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	4041086 (Monthly Rollup) 4040960 (Security Only)	Important	Remote Code Execution	4019115, 4035039, 4014984, 4032116, 4019112, 4035036, 4014981, 4032113 2978128	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	4040977 (Monthly Rollup) 4040960 (Security Only)	Important	Remote Code Execution	4019115, 4035039, 4014984, 4032116, 4019112, 4035036, 4014981, 4032113 2978128	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-8759						
Microsoft .NET Framework 4.5.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4040977 (Monthly Rollup) 4040960 (Security Only)	Important	Remote Code Execution	4019115, 4035039, 4014984, 4032116, 4019112, 4035036, 4014981, 4032113 2978128	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2012	4040975 (Monthly Rollup) 4040959 (Security Only)	Important	Remote Code Execution	4019113, 4035037, 4014982, 4032114 2978127	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2012 (Server Core installation)	4040975 (Monthly Rollup) 4040959 (Security Only)	Important	Remote Code Execution	4019113, 4035037, 4014982, 4032114 2978127	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2012 R2	4040974 (Monthly Rollup) 4040958	Important	Remote Code Execution	4019114, 4035038, 4014983, 4032115 2978126	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-8759						
	(Security Only)					
Microsoft .NET Framework 4.5.2 on Windows Server 2012 R2 (Server Core installation)	4040974 (Monthly Rollup) 4040958 (Security Only)	Important	Remote Code Execution	4019114, 4035038, 4014983, 4032115 2978126	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6 on Windows 10 for 32-bit Systems	4038781 (Security Update)	Important	Remote Code Execution	4034668	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.6 on Windows 10 for x64-based Systems	4038781 (Security Update)	Important	Remote Code Execution	4034668	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.6 on Windows Server 2008 for 32-bit Systems Service Pack 2	4040973 (Monthly Rollup) 4040957	Important	Remote Code Execution	4019115, 4035039, 4014984, 4032116, 4019112, 4035036, 4014981, 4032113	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-8759						
	(Security Only)					
Microsoft .NET Framework 4.6 on Windows Server 2008 for x64-based Systems Service Pack 2	4041086 (Monthly Rollup) 4040957 (Security Only)	Important	Remote Code Execution	4019115, 4035039, 4014984, 4032116, 4019112, 4035036, 4014981, 4032113	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6.1 on Windows 10 Version 1511 for 32-bit Systems	4038783 (Security Update)	Important	Remote Code Execution	4034660	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.6.1 on Windows 10 Version 1511 for x64-based Systems	4038783 (Security Update)	Important	Remote Code Execution	4034660	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.6.2/4.7 on Windows 10 Version 1607 for 32-bit Systems	4038782 (Security Update)	Important	Remote Code Execution	4034658	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2017-8759						
Microsoft .NET Framework 4.6.2/4.7 on Windows 10 Version 1607 for x64-based Systems	4038782 (Security Update)	Important	Remote Code Execution	4034658	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.6.2/4.7 on Windows Server 2016	4038782 (Security Update)	Important	Remote Code Execution	4034658	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.6.2/4.7 on Windows Server 2016 (Server Core installation)	4038782 (Security Update)	Important	Remote Code Execution	4034658	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7 on Windows 7 for 32-bit Systems Service Pack 1	4040973 (Monthly Rollup) 4040957 (Security Only)	Important	Remote Code Execution	4019115, 4035039, 4014984, 4032116, 4019112, 4035036, 4014981, 4032113	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-8759						
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7 on Windows 7 for x64-based Systems Service Pack 1	4040973 (Monthly Rollup) 4040957 (Security Only)	Important	Remote Code Execution	4019115, 4035039, 4014984, 4032116, 4019112, 4035036, 4014981, 4032113	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7 on Windows 8.1 for 32-bit systems	4040972 (Monthly Rollup) 4040956 (Security Only)	Important	Remote Code Execution	4019114, 4035038, 4014983, 4032115	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7 on Windows 8.1 for x64-based systems	4040972 (Monthly Rollup) 4040956 (Security Only)	Important	Remote Code Execution	4019114, 4035038, 4014983, 4032115	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7 on Windows RT 8.1	4040972 (Monthly Rollup)	Important	Remote Code Execution	4019114, 4035038, 4014983, 4032115	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-8759						
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4040973 (Monthly Rollup) 4040957 (Security Only)	Important	Remote Code Execution	4019115, 4035039, 4014984, 4032116, 4019112, 4035036, 4014981, 4032113	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4040973 (Monthly Rollup) 4040957 (Security Only)	Important	Remote Code Execution	4019115, 4035039, 4014984, 4032116, 4019112, 4035036, 4014981, 4032113	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7 on Windows Server 2012	4040971 (Monthly Rollup) 4040955 (Security Only)	Important	Remote Code Execution	4019113, 4035037, 4014982, 4032114	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7 on Windows Server 2012 (Server Core installation)	4040971 (Monthly Rollup) 4040955	Important	Remote Code Execution	4019113, 4035037, 4014982, 4032114	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-8759						
	(Security Only)					
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7 on Windows Server 2012 R2	4040972 (Monthly Rollup) 4040956 (Security Only)	Important	Remote Code Execution	4019114, 4035038, 4014983, 4032115	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7 on Windows Server 2012 R2 (Server Core installation)	4040972 (Monthly Rollup) 4040956 (Security Only)	Important	Remote Code Execution	4019114, 4035038, 4014983, 4032115	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.7 on Windows 10 Version 1703 for 32-bit Systems	4038788 (Security Update)	Important	Remote Code Execution	4034674	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.7 on Windows 10 Version 1703 for x64-based Systems	4038788 (Security Update)	Important	Remote Code Execution	4034674	Base: N/A Temporal: N/A	Yes

CVE-2017-8759						
					Vector: N/A	

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

声　明

==========

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交易，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