Microsoft Security Bulletin Summary for November 2016

Published: November 8, 2016 | Updated: November 23, 2016

Version: 1.1

This bulletin summary lists security bulletins released for November 2016.

For information about how to receive automatic notifications whenever Microsoft security bulletins are issued, visit Microsoft Technical Security Notifications.

Microsoft also provides information to help customers prioritize monthly security updates with any non-security updates that are being released on the same day as the monthly security updates. Please see the section, **Other Information**.

On this page

Executive Summaries

The following table summarizes the security bulletins for this month in order of severity.

For details on affected software, see the next section, **Affected Software**.

Bulletin ID	Bulletin Title and Executive Summary	Maximum Severity Rating and Vulnerability Impact	Restart Requirement	Known Issues	Affected Software
MS16-129	**Cumulative Security Update for Microsoft Edge (3199057)** This security update resolves vulnerabilities in Microsoft Edge. The most severe of the vulnerabilities could allow remote code execution if a user views a specially crafted webpage using Microsoft Edge. An attacker who successfully exploited the vulnerabilities could gain the same user rights as the current user. Customers whose accounts are configured to have fewer user rights on the system could be less impacted than users with administrative user rights.	Critical Remote Code Execution	Requires restart	3200970	Microsoft Windows, Microsoft Edge
MS16-130	**Security Update for Microsoft Windows (3199172)** This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow remote code execution if a locally authenticated attacker runs a specially crafted application.	Critical Remote Code Execution	Requires restart	3197873 3197874 3197876 3197877 3197867 3197868	Microsoft Windows
MS16-131	**Security Update for Microsoft Video Control (3199151)** This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow remote code execution when Microsoft Video Control fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of	Critical Remote Code Execution	Requires restart	3197873 3197874 3197876 3197877 3197867 3197868	Microsoft Windows

	the current user. However, an attacker must first convince a user to open either a specially crafted file or a program from either a webpage or an email message.				
MS16-132	**Security Update for Microsoft Graphics Component (3199120)** This security update resolves vulnerabilities in Microsoft Windows. The most severe being of the vulnerabilities could allow a remote code execution vulnerability exists when the Windows Animation Manager improperly handles objects in memory if a user visits a malicious webpage. An attacker who successfully exploited the vulnerability could install programs; view, change, or delete data; or create new accounts with full user rights.	Critical Remote Code Execution	Requires restart	3197873 3197874 3197876 3197877 3197867 3197868	Microsoft Windows
MS16-133	**Security Update for Microsoft Office (3199168)** This security update resolves vulnerabilities in Microsoft Office. The most severe of the vulnerabilities could allow remote code execution if a user opens a specially crafted Microsoft Office file. An attacker who successfully exploited the vulnerabilities could run arbitrary code in the context of the current user. Customers whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.	Important Remote Code Execution	May require restart	---------	Microsoft Office, Microsoft Office Services and Web Apps
MS16-134	**Security Update for Common Log File System Driver (3193706)** This security update resolves vulnerabilities in Microsoft Windows. The vulnerability could allow elevation of privilege when the Windows Common Log File System (CLFS) driver improperly handles objects in memory. In a local attack scenario, an attacker could exploit these vulnerabilities by running a specially crafted application to take complete control over the affected system. An attacker who successfully exploits this vulnerability could run processes in an elevated context.	Important Elevation of Privilege	Requires restart	3197873 3197874 3197876 3197877 3197867 3197868	Microsoft Windows
MS16-135	**Security Update for Windows Kernel-Mode Drivers (3199135)** This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow elevation of privilege if an attacker logs on to an affected system and runs a specially crafted application that could exploit the vulnerabilities and take control of an affected system.	Important Elevation of Privilege	Requires restart	3197873 3197874 3197876 3197877 3197867 3197868	Microsoft Windows
MS16-136	**Security Update for SQL Server (3199641)** This security update resolves vulnerabilities in Microsoft SQL Server. The most severe vulnerabilities could allow an attacker could to gain elevated privileges that could be	Important Elevation of Privilege	May require restart	---------	Microsoft SQL Server

	used to view, change, or delete data; or create new accounts. The security update addresses these most severe vulnerabilities by correcting how SQL Server handles pointer casting.				
MS16-137	**Security Update for Windows Authentication Methods (3199173)** This security update resolves vulnerabilities in Microsoft Windows. The more severe of the vulnerabilities could allow elevation of privilege. To exploit this vulnerability, the attacker would first need to authenticate to the target, domain-joined system using valid user credentials. An attacker who successfully exploited this vulnerability could elevate their permissions from unprivileged user account to administrator. The attacker could then install programs; view, change or delete data; or create new accounts. The attacker could subsequently attempt to elevate by locally executing a specially crafted application designed to manipulate NTLM password change requests.	Important Elevation of Privilege	Requires restart	3197873 3197874 3197876 3197877 3197867 3197868	Microsoft Windows
MS16-138	**Security Update to Microsoft Virtual Hard Disk Driver (3199647)** This security update resolves vulnerabilities in Microsoft Windows. The Windows Virtual Hard Disk Driver improperly handles user access to certain files. An attacker could manipulate files in locations not intended to be available to the user by exploiting this vulnerability.	Important Elevation of Privilege	Requires restart	3197873 3197874 3197876 3197877	Microsoft Windows
MS16-139	**Security Update for Windows Kernel (3199720)** This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if an attacker runs a specially crafted application to access sensitive information. A locally authenticated attacker could attempt to exploit this vulnerability by running a specially crafted application. An attacker can gain access to information not intended to be available to the user by using this method.	Important Elevation of Privilege	Requires restart	3197867 3197868	Microsoft Windows
MS16-140	**Security Update for Boot Manager (3193479)** This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow security feature bypass if a physically-present attacker installs an affected boot policy.	Important Security Feature Bypass	Requires restart	3200970 3197877 3197876 3197874 3197873 3193479	Microsoft Windows
MS16-141	**Security Update for Adobe Flash Player (3202790)** This security update resolves vulnerabilities in Adobe Flash Player when installed on all supported editions of Windows 8.1, Windows Server 2012, Windows Server 2012 R2, Windows RT 8.1, Windows 10, and Windows Server 2016.	Critical Remote Code Execution	Requires restart	---------	Microsoft Windows, Adobe Flash Player

MS16-142	**Cumulative Security Update for Internet Explorer (3198467)** This security update resolves vulnerabilities in Internet Explorer. The most severe of the vulnerabilities could allow remote code execution if a user views a specially crafted webpage using Internet Explorer. An attacker who successfully exploited the vulnerabilities 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	Requires restart	3197873 3197874 3197876 3197877 3197867 3197868	Microsoft Windows, Internet Explorer

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

How do I use this table?

Use this table to learn about the likelihood of code execution and denial of service exploits within 30 days of security bulletin release, for each of the security updates that you may need to install. Review each of the assessments below, in accordance with your specific configuration, to prioritize your deployment of this month's updates. For more information about what these ratings mean, and how they are determined, please see Microsoft Exploitability Index.

In the columns below, "Latest Software Release" refers to the subject software, and "Older Software Releases" refers to all older, supported releases of the subject software, as listed in the "Affected Software" and "Non-Affected Software" tables in the bulletin.

CVE ID	Vulnerability Title	Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment
MS16-129: Cumulative Security Update for Microsoft Edge (3199057)				
CVE-2016-7195	Microsoft Browser Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-7196	Microsoft Browser Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-7198	Microsoft Browser Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-7199	Microsoft Browser Information Disclosure Vulnerability	2 - Exploitation Less Likely	4 - Not affected	Not applicable
CVE-2016-7200	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable

CVE-2016-7201	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-7202	Scripting Engine Memory Corruption Vulnerability	4 - Not affected	4 - Not affected	Not applicable
CVE-2016-7203	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-7204	Microsoft Edge Information Disclosure Vulnerability	2 - Exploitation Less Likely	4 - Not affected	Not applicable
CVE-2016-7208	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-7209	Microsoft Edge Spoofing Vulnerability	2 - Exploitation Less Likely	4 - Not affected	Not applicable
CVE-2016-7227	Microsoft Browser Information Disclosure Vulnerability	2 - Exploitation Less Likely	4 - Not affected	Not applicable
CVE-2016-7239	Microsoft Browser Information Disclosure	3 - Exploitation Unlikely	4 - Not affected	Not applicable
CVE-2016-7240	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-7241	Microsoft Browser Remote Code Execution Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-7242	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-7243	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
MS16-130: Security Update for Microsoft Windows (3199172)				
CVE-2016-7212	Windows Remote Code Execution Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2016-7221	Windows IME	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable

	Elevation of Privilege Vulnerability			
CVE-2016-7222	Task Scheduler Elevation of Privilege Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Permanent
MS16-131: Security Update for Microsoft Video Control (3199151)				
CVE-2016-7248	Security Update for Microsoft Video Control	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
MS16-132: Security Update for Microsoft Graphics Component (3199120)				
CVE-2016-7205	Windows Animation Manager Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-7210	Open Type Font Information Disclosure Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2016-7217	Media Foundation Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-7256	Open Type Font Remote Code Execution Vulnerability	2 - Exploitation Less Likely	0 - Exploitation Detected	Not applicable
MS16-133: Security Update for Microsoft Office (3199168)				
CVE-2016-7213	Microsoft Office Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-7228	Microsoft Office Memory Corruption Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2016-7229	Microsoft Office Memory Corruption Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2016-7230	Microsoft Office Memory Corruption Vulnerability	4 - Not affected	1 - Exploitation More Likely	Not applicable
CVE-2016-7231	Microsoft Office Memory Corruption Vulnerability	4 - Not affected	2 - Exploitation Less Likely	Not applicable

CVE-2016-7232	Microsoft Office Memory Corruption Vulnerability	4 - Not affected	2 - Exploitation Less Likely	Not applicable
CVE-2016-7233	Microsoft Office Information Disclosure Vulnerability	4 - Not affected	2 - Exploitation Less Likely	Not applicable
CVE-2016-7234	Microsoft Office Memory Corruption Vulnerability	4 - Not affected	2 - Exploitation Less Likely	Not applicable
CVE-2016-7235	Microsoft Office Memory Corruption Vulnerability	4 - Not affected	2 - Exploitation Less Likely	Not applicable
CVE-2016-7236	Microsoft Office Memory Corruption Vulnerability	4 - Not affected	2 - Exploitation Less Likely	Not applicable
CVE-2016-7244	Microsoft Office Denial of Service Vulnerability	4 - Not affected	3 - Exploitation Unlikely	Not applicable
CVE-2016-7245	Microsoft Office Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
MS16-134: Security Update for Common Log File System Driver (3193706)				
CVE-2016-0026	Windows CLFS Elevation of Privilege	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2016-3332	Windows Common Log File System Driver Elevation of Privilege Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2016-3333	Windows Common Log File System Driver Elevation of Privilege Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2016-3334	Windows Common Log File System Driver Elevation of Privilege Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2016-3335	Windows Common Log File System Driver Elevation of	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable

	Privilege Vulnerability			
CVE-2016-3338	Windows Common Log File System Driver Elevation of Privilege Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2016-3340	Windows Common Log File System Driver Elevation of Privilege Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2016-3342	Windows Common Log File System Driver Elevation of Privilege Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2016-3343	Windows Common Log File System Driver Elevation of Privilege Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2016-7184	Windows CLFS Elevation of Privilege	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
MS16-135: Security Update for Windows Kernel-Mode Drivers (3199135)				
CVE-2016-7214	Win32k Information Disclosure Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2016-7215	Win32k Elevation of Privilege Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Permanent
CVE-2016-7218	Bowser.sys Information Disclosure Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2016-7246	Win32k Elevation of Privilege Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-7255	Win32k Elevation of Privilege Vulnerability	1 - Exploitation More Likely	0 - Exploitation Detected	Not applicable
MS16-136: Security Update for SQL Server (3199641)				
CVE-2016-7249	SQL RDBMS Engine Elevation of Privilege Vulnerability	3 - Exploitation Unlikely	4 - Not affected	Not applicable

CVE-2016-7250	SQL RDBMS Engine Elevation of Privilege Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2016-7251	MDS API XSS Vulnerability	3 - Exploitation Unlikely	4 - Not affected	Not applicable
CVE-2016-7252	SQL Analysis Services Information Disclosure Vulnerability	3 - Exploitation Unlikely	4 - Not affected	Not applicable
CVE-2016-7253	SQL Server Agent Elevation of Privilege Vulnerability	4 - Not affected	3 - Exploitation Unlikely	Not applicable
CVE-2016-7254	SQL RDBMS Engine EoP vulnerability	4 - Not affected	2 - Exploitation Less Likely	Not applicable
MS16-137:Security Update for Windows Authentication Methods (3199173)				
CVE-2016-7220	Virtual Secure Mode Information Disclosure Vulnerability	4 - Not affected	2 - Exploitation Less Likely	Not applicable
CVE-2016-7237	Local Security Authority Subsystem Service Denial of Service Vulnerability	3 - Exploitation Unlikely	3 - Exploitation Unlikely	Permanent
CVE-2016-7238	Windows NTLM elevation of privilege vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
MS16-138: Security Update to Microsoft Virtual Hard Disk Driver (3199647)				
CVE-2016-7223	VHDFS Driver Elevation of Privilege Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2016-7224	VHDFS Driver Elevation of Privilege Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2016-7225	VHDFS Driver Elevation of Privilege Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Permanent
CVE-2016-7226	VHDFS Driver Elevation of Privilege Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
MS16-139: Security Update for Windows Kernel (3199720)				

CVE-2016-7216	Windows Kernel Elevation of Privilege Vulnerability	4 - Not affected	2 - Exploitation Less Likely	Not applicable
MS16-140: Security Update for Boot Manager (3193479)				
CVE-2016-7247	Secure Boot Security Feature Bypass Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
MS16-141: Security Update for Adobe Flash Player (3202790)				
APSB16-37	See Adobe Security Bulletin APSB16-37 for vulnerability severity and update priority ratings.	---	---	Not applicable
MS16-142: Cumulative Security Update for Internet Explorer (3198467)				
CVE-2016-7239	Microsoft Browser Information Disclosure	3 - Exploitation Unlikely	3 - Exploitation Unlikely	Not applicable
CVE-2016-7227	Microsoft Browser Information Disclosure Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-7198	Microsoft Browser Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-7199	Microsoft Browser Information Disclosure Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2016-7195	Microsoft Browser Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-7196	Microsoft Browser Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-7241	Microsoft Browser Remote Code Execution Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable

Affected Software

The following tables list the bulletins in order of major software category and severity.

Use these tables to learn about the security updates that you may need to install. You should review each software program or component listed to see whether any security updates pertain to your installation. If a software program or component is listed, then the severity rating of the software update is also listed.

Note You may have to install several security updates for a single vulnerability. Review the whole column for each bulletin identifier that is listed to verify the updates that you have to install, based on the programs or components that you have installed on your system.

Windows Operating Systems and Components (Table 1 of 3)

Windows Vista				
Bulletin Identifier	**MS16-129**	**MS16-130**	**MS16-131**	**MS16-132**
Aggregate Severity Rating	**None**	**Critical**	**Critical**	**Critical**
Windows Vista Service Pack 2	Not applicable	Windows Vista Service Pack 2 (3193418) (Important) Windows Vista Service Pack 2 (3196718) (Critical)	Windows Vista Service Pack 2 (3198218) (Critical)	Windows Vista Service Pack 2 (3203859) (Important)
Windows Vista x64 Edition Service Pack 2	Not applicable	Windows Vista x64 Edition Service Pack 2 (3193418) (Important) Windows Vista x64 Edition Service Pack 2 (3196718) (Critical)	Windows Vista x64 Edition Service Pack 2 (3198218) (Critical)	Windows Vista x64 Edition Service Pack 2 (3203859) (Important)
Windows Server 2008				
Bulletin Identifier	**MS16-129**	**MS16-130**	**MS16-131**	**MS16-132**
Aggregate Severity Rating	**None**	**Critical**	**None**	**Critical**
Windows Server 2008 for 32-bit Systems Service Pack 2	Not applicable	Windows Server 2008 for 32-bit Systems Service Pack 2 (3193418) (Important) Windows Server 2008 for 32-bit Systems Service Pack 2 (3196718) (Critical)	Not applicable	Windows Server 2008 for 32-bit Systems Service Pack 2 (3203859) (Important)
Windows Server 2008 for x64-based Systems Service Pack 2	Not applicable	Windows Server 2008 for x64-based Systems Service Pack 2 (3193418) (Critical) Windows Server 2008 for x64-based Systems Service Pack 2	Not applicable	Windows Server 2008 for x64-based Systems Service Pack 2 (3203859) (Important)

		(3196718) (Critical)		
Windows Server 2008 for Itanium-based Systems Service Pack 2	Not applicable	Windows Server 2008 for Itanium-based Systems Service Pack 2 (3193418) (Important) Windows Server 2008 for Itanium-based Systems Service Pack 2 (3196718) (Critical)	Not applicable	Windows Server 2008 for Itanium-based Systems Service Pack 2 (3203859) (Important)
Windows 7				
Bulletin Identifier	**MS16-129**	**MS16-130**	**MS16-131**	**MS16-132**
Aggregate Severity Rating	**None**	**Critical**	**Critical**	**Critical**
Windows 7 for 32-bit Systems Service Pack 1 Security Only	Not applicable	Windows 7 for 32-bit Systems Service Pack 1 (3197867) (Critical)	Windows 7 for 32-bit Systems Service Pack 1 (3197867) (Critical)	Windows 7 for 32-bit Systems Service Pack 1 (3197867) (Critical)
Windows 7 for 32-bit Systems Service Pack 1 Monthly Roll Up	Not applicable	Windows 7 for 32-bit Systems Service Pack 1 (3197868) (Critical)	Windows 7 for 32-bit Systems Service Pack 1 (3197868) (Critical)	Windows 7 for 32-bit Systems Service Pack 1 (3197868) (Critical)
Windows 7 for x64-based Systems Service Pack 1 Security Only	Not applicable	Windows 7 for x64-based Systems Service Pack 1 (3197867) (Critical)	Windows 7 for x64-based Systems Service Pack 1 (3197867) (Critical)	Windows 7 for x64-based Systems Service Pack 1 (3197867) (Critical)
Windows 7 for x64-based Systems Service Pack 1 Monthly Roll Up	Not applicable	Windows 7 for x64-based Systems Service Pack 1 (3197868) (Critical)	Windows 7 for x64-based Systems Service Pack 1 (3197868) (Critical)	Windows 7 for x64-based Systems Service Pack 1 (3197868) (Critical)
Windows Server 2008 R2				
Bulletin Identifier	**MS16-129**	**MS16-130**	**MS16-131**	**MS16-132**
Aggregate Severity Rating	**None**	**Critical**	**None**	**Critical**
Windows Server 2008 R2 for x64-based Systems Service Pack 1 Security Only	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3197867) (Critical)	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3197867) (Critical)
Windows Server 2008 R2 for x64-based Systems Service Pack 1 Monthly Roll Up	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1

		(3197868) (Critical)		(3197868) (Critical)
Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 Security Only	Not applicable	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3197867) (Critical)	Not applicable	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3197867) (Critical)
Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 Monthly Rollup	Not applicable	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3197868) (Critical)	Not applicable	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3197868) (Critical)
Windows 8.1				
Bulletin Identifier	**MS16-129**	**MS16-130**	**MS16-131**	**MS16-132**
Aggregate Severity Rating	**None**	**Critical**	**Critical**	**Critical**
Windows 8.1 for 32-bit Systems Security Only	Not applicable	Windows 8.1 for 32-bit Systems (3197873) (Critical)	Windows 8.1 for 32-bit Systems (3197873) (Important)	Windows 8.1 for 32-bit Systems (3197873) (Critical)
Windows 8.1 for 32-bit Systems Monthly Roll Up	Not applicable	Windows 8.1 for 32-bit Systems (3197874) (Critical)	Windows 8.1 for 32-bit Systems (3197874) (Important)	Windows 8.1 for 32-bit Systems (3197874) (Critical)
Windows 8.1 for x64-based Systems Security Only	Not applicable	Windows 8.1 for x64-based Systems (3197873) (Critical)	Windows 8.1 for x64-based Systems (3197873) (Important)	Windows 8.1 for x64-based Systems (3197873) (Critical)
Windows 8.1 for x64-based Systems Monthly Roll Up	Not applicable	Windows 8.1 for x64-based Systems (3197874) (Critical)	Windows 8.1 for x64-based Systems (3197874) (Important)	Windows 8.1 for x64-based Systems (3197874) (Critical)
Windows Server 2012 and Windows Server 2012 R2				
Bulletin Identifier	**MS16-129**	**MS16-130**	**MS16-131**	**MS16-132**
Aggregate Severity Rating	**None**	**Critical**	**None**	**Critical**
Windows Server 2012 Security Only	Not applicable	Windows Server 2012 (3197876) (Critical)	Not applicable	Windows Server 2012 (3197876) (Critical)
Windows Server 2012 Monthly Roll Up	Not applicable	Windows Server 2012 (3197877) (Critical)	Not applicable	Windows Server 2012 (3197877) (Critical)
Windows Server 2012 R2 Security Only	Not applicable	Windows Server 2012 R2 (3197873) (Critical)	Not applicable	Windows Server 2012 R2 (3197873) (Critical)

Windows Server 2012 R2 Monthly Roll Up	Not applicable	Windows Server 2012 R2 (3197874) (Critical)	Not applicable	Windows Server 2012 R2 (3197874) (Critical)
Windows RT 8.1				
Bulletin Identifier	**MS16-129**	**MS16-130**	**MS16-131**	**MS16-132**
Aggregate Severity Rating	**None**	**Critical**	**Critical**	**Critical**
Windows RT 8.1 Monthly Roll Up	Not applicable	Windows RT 8.1 (3197874) (Critical)	Windows RT 8.1 (3197874) (Critical)	Windows RT 8.1 (3197874) (Important)
Windows 10				
Bulletin Identifier	**MS16-129**	**MS16-130**	**MS16-131**	**MS16-132**
Aggregate Severity Rating	**Critical**	**Critical**	**Critical**	**Critical**
Windows 10 for 32-bit Systems	Windows 10 for 32-bit Systems (3198585) (Critical)	Windows 10 for 32-bit Systems (3198585) (Critical)	Windows 10 for 32-bit Systems (3198585) (Critical)	Windows 10 for 32-bit Systems (3198585) (Important)
Windows 10 for 32-bit Systems (3198585)	Windows 10 for x64-based Systems (3198585) (Critical)	Windows 10 for x64-based Systems (3198585) (Critical)	Windows 10 for x64-based Systems (3198585) (Critical)	Windows 10 for x64-based Systems (3198585) (Important)
Windows 10 for x64-based Systems (3198585)	Windows 10 Version 1511 for 32-bit Systems (3198586) (Critical)	Windows 10 Version 1511 for 32-bit Systems (3198586) (Critical)	Windows 10 Version 1511 for 32-bit Systems (3198586) (Critical)	Windows 10 Version 1511 for 32-bit Systems (3198586) (Important)
Windows 10 Version 1511 for 32-bit Systems (3198586)	Windows 10 Version 1511 for x64-based Systems (3198586) (Critical)	Windows 10 Version 1511 for x64-based Systems (3198586) (Critical)	Windows 10 Version 1511 for x64-based Systems (3198586) (Critical)	Windows 10 Version 1511 for x64-based Systems (3198586) (Important)
Windows 10 Version 1511 for x64-based Systems (3198586)	Windows 10 Version 1607 for 32-bit Systems (3200970) (Critical)	Windows 10 Version 1607 for 32-bit Systems (3200970) (Critical)	Windows 10 Version 1607 for 32-bit Systems (3200970) (Critical)	Windows 10 Version 1607 for 32-bit Systems (3200970) (Important)
Windows 10 Version 1607 for 32-bit Systems (3200970)	Windows 10 Version 1607 for x64-based Systems (3200970) (Critical)	Windows 10 Version 1607 for x64-based Systems (3200970) (Critical)	Windows 10 Version 1607 for x64-based Systems (3200970) (Critical)	Windows 10 Version 1607 for x64-based Systems (3200970) (Important)
Windows Server 2016				

Bulletin Identifier	**MS16-129**	**MS16-130**	**MS16-131**	**MS16-132**
Aggregate Severity Rating	**None**	**Critical**	**None**	**Critical**
Windows Server 2016 for x64-based Systems	Not applicable	Windows Server 2016 for x64-based Systems (3200970) (Critical)	Not applicable	Windows Server 2016 for x64-based Systems (3200970) (Critical)
Server Core installation option				
Bulletin Identifier	**MS16-129**	**MS16-130**	**MS16-131**	**MS16-132**
Aggregate Severity Rating	**None**	**Critical**	**None**	**Critical**
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	Not applicable	Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (3193418) (Important) Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (3196718) (Critical)	Not applicable	Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (3203859) (Important)
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	Not applicable	Windows Server 2008 for x86-bit Systems Service Pack 2 (Server Core installation) (3193418) (Important) Windows Server 2008 for x86-bit Systems Service Pack 2 (Server Core installation) (3196718) (Critical)	Not applicable	Windows Server 2008 for x86-bit Systems Service Pack 2 (Server Core installation) (3203859) (Important)
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) Security Only	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3197867) (Critical)	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3197867) (Critical)
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) Monthly Rollup	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3197868) (Critical)	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3197868) (Critical)
Windows Server 2012 (Server Core installation) Security Only	Not applicable	Windows Server 2012 (Server Core installation) (3197876) (Critical)	Not applicable	Windows Server 2012 (Server Core installation) (3197876) (Critical)
Windows Server 2012 (Server Core installation) Monthly Rollup	Not applicable	Windows Server 2012 (Server Core installation)	Not applicable	Windows Server 2012 (Server Core installation)

		(3197877) (Critical)		(3197877) (Critical)
Windows Server 2012 R2 (Server Core installation) Security Only	Not applicable	Windows Server 2012 R2 (Server Core installation) (3197873) (Critical)	Not applicable	Windows Server 2012 R2 (Server Core installation) (3197873) (Critical)
Windows Server 2012 R2 (Server Core installation) Monthly Rollup	Not applicable	Windows Server 2012 R2 (Server Core installation) (3197874) (Critical)	Not applicable	Windows Server 2012 R2 (Server Core installation) (3197874) (Critical)
Windows Server 2016 for x64-based Systems (Server Core installation)	Not applicable	Windows Server 2016 for x64-based Systems (Server Core installation) (3200970) (Critical)	Not applicable	Windows Server 2016 for x64-based Systems (Server Core installation) (3200970) (Critical)

Windows Operating Systems and Components (Table 2 of 3)

Windows Vista					
Bulletin Identifier	**MS16-134**	**MS16-135**	**MS16-137**	**MS16-138**	**MS16-139**
Aggregate Severity Rating	**Important**	**Important**	**Important**	**None**	**Important**
Windows Vista Service Pack 2	Windows Vista Service Pack 2 (3181707) (Important)	Windows Vista Service Pack 2 (3198234) (Important) Windows Vista Service Pack 2 (3194371) (Important)	Windows Vista Service Pack 2 (3198510) (Important)	Not applicable	Windows Vista Service Pack 2 (3198483) (Important)
Windows Vista x64 Edition Service Pack 2	Windows Vista x64 Edition Service Pack 2 (3181707) (Important)	Windows Vista x64 Edition Service Pack 2 (3198234) (Important) Windows Vista x64 Edition Service Pack 2 (3194371) (Important)	Windows Vista x64 Edition Service Pack 2 (3198510) (Important)	Not applicable	Windows Vista x64 Edition Service Pack 2 (3198483) (Important)
Windows Server 2008					
Bulletin Identifier	**MS16-134**	**MS16-135**	**MS16-137**	**MS16-138**	**MS16-139**
Aggregate Severity Rating	**Important**	**Important**	**Important**	**None**	**Important**
Windows Server 2008 for 32-bit Systems Service Pack 2	Windows Server 2008 for 32-bit Systems Service Pack 2 (3181707) (Important)	Windows Server 2008 for 32-bit Systems Service Pack 2 (3198234) (Important)	Windows Server 2008 for 32-bit Systems Service Pack 2 (3198510) (Important)	Not applicable	Windows Server 2008 for 32-bit Systems Service Pack 2 (3198483) (Important)

		Windows Server 2008 for 32-bit Systems Service Pack 2 (3194371) (Important)			
Windows Server 2008 for x64-based Systems Service Pack 2	Windows Server 2008 for x64-based Systems Service Pack 2 (3181707) (Important)	Windows Server 2008 for x64-based Systems Service Pack 2 (3198234) (Important) Windows Server 2008 for x64-based Systems Service Pack 2 (3194371) (Important)	Windows Server 2008 for x64-based Systems Service Pack 2 (3198510) (Important)	Not applicable	Windows Server 2008 for x64-based Systems Service Pack 2 (3198483) (Important)
Windows Server 2008 for Itanium-based Systems Service Pack 2	Windows Server 2008 for Itanium-based Systems Service Pack 2 (3181707) (Important)	Windows Server 2008 for Itanium-based Systems Service Pack 2 (3198234) (Important) Windows Server 2008 for Itanium-based Systems Service Pack 2 (3194371) (Important)	Windows Server 2008 for Itanium-based Systems Service Pack 2 (3198510) (Important)	Not applicable	Windows Server 2008 for Itanium-based Systems Service Pack 2 (3198483) (Important)
Windows 7					
Bulletin Identifier	**MS16-134**	**MS16-135**	**MS16-137**	**MS16-138**	**MS16-139**
Aggregate Severity Rating	**Important**	**Important**	**Important**	**None**	**Important**
Windows 7 for 32-bit Systems Service Pack 1 Security Only	Windows 7 for 32-bit Systems Service Pack 1 (3197867) (Important)	Windows 7 for 32-bit Systems Service Pack 1 (3197867) (Important)	Windows 7 for 32-bit Systems Service Pack 1 (3197867) (Important)	Not applicable	Windows 7 for 32-bit Systems Service Pack 1 (3197867) (Important)
Windows 7 for 32-bit Systems Service Pack 1 Monthly Roll Up	Windows 7 for 32-bit Systems Service Pack 1 (3197868) (Important)	Windows 7 for 32-bit Systems Service Pack 1 (3197868) (Important)	Windows 7 for 32-bit Systems Service Pack 1 (3197868) (Important)	Not applicable	Windows 7 for 32-bit Systems Service Pack 1 (3197868) (Important)
Windows 7 for x64-based Systems Service Pack 1 Security Only	Windows 7 for x64-based Systems Service Pack 1 (3197867) (Important)	Windows 7 for x64-based Systems Service Pack 1 (3197867) (Important)	Windows 7 for x64-based Systems Service Pack 1 (3197867) (Important)	Not applicable	Windows 7 for x64-based Systems Service Pack 1 (3197867) (Important)
Windows 7 for x64-based Systems Service Pack 1	Windows 7 for x64-based	Windows 7 for x64-based	Windows 7 for x64-based	Not applicable	Windows 7 for x64-based

Monthly Roll Up	Systems Service Pack 1 (3197868) (Important)	Systems Service Pack 1 (3197868) (Important)	Systems Service Pack 1 (3197868) (Important)		Systems Service Pack 1 (3197868) (Important)
Windows Server 2008 R2					
Bulletin Identifier	**MS16-134**	**MS16-135**	**MS16-137**	**MS16-138**	**MS16-139**
Aggregate Severity Rating	**Important**	**Important**	**Important**	**None**	**Important**
Windows Server 2008 R2 for x64-based Systems Service Pack 1 Security Only	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3197867) (Important)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3197867) (Important)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3197867) (Important)	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3197867) (Important)
Windows Server 2008 R2 for x64-based Systems Service Pack 1 Monthly Roll Up	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3197868) (Important)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3197868) (Important)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3197868) (Important)	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3197868) (Important)
Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 Security Only	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3197867) (Important)	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3197867) (Important)	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3197867) (Important)	Not applicable	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3197867) (Important)
Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 Monthly Rollup	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3197868) (Important)	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3197868) (Important)	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3197868) (Important)	Not applicable	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3197868) (Important)
Windows 8.1					
Bulletin Identifier	**MS16-134**	**MS16-135**	**MS16-137**	**MS16-138**	**MS16-139**
Aggregate Severity Rating	**Important**	**Important**	**Important**	**Important**	**None**
Windows 8.1 for 32-bit Systems Security Only	Windows 8.1 for 32-bit Systems (3197873) (Important)	Windows 8.1 for 32-bit Systems (3197873) (Important)	Windows 8.1 for 32-bit Systems (3197873) (Important)	Windows 8.1 for 32-bit Systems (3197873) (Important)	Not applicable
Windows 8.1 for 32-bit Systems Monthly Roll Up	Windows 8.1 for 32-bit Systems (3197874) (Important)	Windows 8.1 for 32-bit Systems (3197874) (Important)	Windows 8.1 for 32-bit Systems (3197874) (Important)	Windows 8.1 for 32-bit Systems (3197874) (Important)	Not applicable
Windows 8.1 for x64-based Systems Security Only	Windows 8.1 for x64-based Systems	Windows 8.1 for x64-based Systems	Windows 8.1 for x64-based Systems	Windows 8.1 for x64-based Systems	Not applicable

	(3197873) (Important)	(3197873) (Important)	(3197873) (Important)	(3197873) (Important)	
Windows 8.1 for x64-based Systems Monthly Roll Up	Windows 8.1 for x64-based Systems (3197874) (Important)	Windows 8.1 for x64-based Systems (3197874) (Important)	Windows 8.1 for x64-based Systems (3197874) (Important)	Windows 8.1 for x64-based Systems (3197874) (Important)	Not applicable
Windows Server 2012 and Windows Server 2012 R2					
Bulletin Identifier	**MS16-134**	**MS16-135**	**MS16-137**	**MS16-138**	**MS16-139**
Aggregate Severity Rating	**Important**	**Important**	**Important**	**Moderate**	**None**
Windows Server 2012 Security Only	Windows Server 2012 (3197876) (Important)	Windows Server 2012 (3197876) (Important)	Windows Server 2012 (3197876) (Important)	Windows Server 2012 (3197876) (Important)	Not applicable
Windows Server 2012 Monthly Roll Up	Windows Server 2012 (3197877) (Important)	Windows Server 2012 (3197877) (Important)	Windows Server 2012 (3197877) (Important)	Windows Server 2012 (3197877) (Important)	Not applicable
Windows Server 2012 R2 Security Only	Windows Server 2012 R2 (3197873) (Important)	Windows Server 2012 R2 (3197873) (Important)	Windows Server 2012 R2 (3197873) (Important)	Windows Server 2012 R2 (3197873) (Important)	Not applicable
Windows Server 2012 R2 Monthly Roll Up	Windows Server 2012 R2 (3197874) (Important)	Windows Server 2012 R2 (3197874) (Important)	Windows Server 2012 R2 (3197874) (Important)	Windows Server 2012 R2 (3197874) (Important)	Not applicable
Windows RT 8.1					
Bulletin Identifier	**MS16-134**	**MS16-135**	**MS16-137**	**MS16-138**	**MS16-139**
Aggregate Severity Rating	**Important**	**Important**	**Important**	**None**	**None**
Windows RT 8.1 Monthly Roll Up	Windows RT 8.1 (3197874) (Important)	Windows RT 8.1 (3197874) (Important)	Windows RT 8.1 (3197874) (Important)	Not applicable	Not applicable
Windows 10					
Bulletin Identifier	**MS16-134**	**MS16-135**	**MS16-137**	**MS16-138**	**MS16-139**
Aggregate Severity Rating	**Important**	**Important**	**Important**	**Important**	**None**
Windows 10 for 32-bit Systems	Windows 10 for 32-bit Systems (3198585) (Important)	Windows 10 for 32-bit Systems (3198585) (Important)	Windows 10 for 32-bit Systems (3198585) (Important)	Windows 10 for 32-bit Systems (3198585) (Important)	Not applicable
Windows 10 for x64-based Systems	Windows 10 for x64-based	Windows 10 for x64-based	Windows 10 for x64-based	Windows 10 for x64-based	Not applicable

	Systems (3198585) (Important)	Systems (3198585) (Important)	Systems (3198585) (Important)	Systems (3198585) (Important)	
Windows 10 Version 1511 for 32-bit Systems	Windows 10 Version 1511 for 32-bit Systems (3198586) (Important)	Windows 10 Version 1511 for 32-bit Systems (3198586) (Important)	Windows 10 Version 1511 for 32-bit Systems (3198586) (Important)	Windows 10 Version 1511 for 32-bit Systems (3198586) (Important)	Not applicable
Windows 10 Version 1511 for x64-based Systems	Windows 10 Version 1511 for x64-based Systems (3198586) (Important)	Windows 10 Version 1511 for x64-based Systems (3198586) (Important)	Windows 10 Version 1511 for x64-based Systems (3198586) (Important)	Windows 10 Version 1511 for x64-based Systems (3198586) (Important)	Not applicable
Windows 10 Version 1607 for 32-bit Systems	Windows 10 Version 1607 for 32-bit Systems (3200970) (Important)	Windows 10 Version 1607 for 32-bit Systems (3200970) (Important)	Windows 10 Version 1607 for 32-bit Systems (3200970) (Important)	Windows 10 Version 1607 for 32-bit Systems (3200970) (Important)	Not applicable
Windows 10 Version 1607 for x64-based Systems	Windows 10 Version 1607 for x64-based Systems (3200970) (Important)	Windows 10 Version 1607 for x64-based Systems (3200970) (Important)	Windows 10 Version 1607 for x64-based Systems (3200970) (Important)	Windows 10 Version 1607 for x64-based Systems (3200970) (Important)	Not applicable
Windows Server 2016					
Bulletin Identifier	**MS16-134**	**MS16-135**	**MS16-137**	**MS16-138**	**MS16-139**
Aggregate Severity Rating	**Important**	**Important**	**Important**	**Important**	**None**
Windows Server 2016 for x64-based Systems	Windows Server 2016 for x64-based Systems (3200970) (Important)	Windows Server 2016 for x64-based Systems (3200970) (Important)	Windows Server 2016 for x64-based Systems (3200970) (Important)	Windows Server 2016 for x64-based Systems (3200970) (Important)	Not applicable
Server Core installation option					
Bulletin Identifier	**MS16-134**	**MS16-135**	**MS16-137**	**MS16-138**	**MS16-139**
Aggregate Severity Rating	**Important**	**Important**	**Important**	**Important**	**Important**
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (3181707) (Important)	Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (3198234) (Important)	Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (3190847) (Important)	Not applicable	Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (3196718) (Important)
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	Windows Server 2008 for x64-based Systems	Windows Server 2008 for x64-based Systems	Windows Server 2008 for x64-based Systems	Not applicable	Windows Server 2008 for x64-based Systems

	Service Pack 2 (Server Core installation) (3181707) (Important)	Service Pack 2 (Server Core installation) (3198234) (Important)	Service Pack 2 (Server Core installation) (3190847) (Important)		Service Pack 2 (Server Core installation) (3196718) (Important)
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) Security Only	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3197867) (Important)	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3197867) (Important)	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3197867) (Important)
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) Monthly Rollup	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3197868) (Important)	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3197868) (Important)	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3197868) (Important)
Windows Server 2012 (Server Core installation) Security Only	Windows Server 2012 (Server Core installation) (3197876) (Important)	Not applicable	Windows Server 2012 (Server Core installation) (3197876) (Important)	Windows Server 2012 (Server Core installation) (3197876) (Important)	Not applicable
Windows Server 2012 (Server Core installation) Monthly Rollup	Windows Server 2012 (Server Core installation) (3197877) (Important)	Not applicable	Windows Server 2012 (Server Core installation) (3197877) (Important)	Windows Server 2012 (Server Core installation) (3197877) (Important)	Not applicable
Windows Server 2012 R2 (Server Core installation) Security Only	Windows Server 2012 R2 (Server Core installation) (3197873) (Important)	Not applicable	Windows Server 2012 R2 (Server Core installation) (3197873) (Important)	Windows Server 2012 R2 (Server Core installation) (3197873) (Important)	Not applicable
Windows Server 2012 R2 (Server Core installation) Monthly Rollup	Windows Server 2012 R2 (Server Core installation) (3197874) (Important)	Not applicable	Windows Server 2012 R2 (Server Core installation) (3197874) (Important)	Windows Server 2012 R2 (Server Core installation) (3197874) (Important)	Not applicable
Windows Server 2016 for x64-based Systems (Server Core installation)	Windows Server 2016 for x64-based Systems (Server Core installation) (3200970) (Important)	Windows Server 2016 for x64-based Systems (Server Core installation) (3200970) (Important)	Windows Server 2016 for x64-based Systems (Server Core installation) (3200970) (Important)	Windows Server 2016 for x64-based Systems (Server Core installation) (3200970) (Important)	Not applicable

Windows Operating Systems and Components (Table 3 of 3)

Windows Vista			
Bulletin Identifier	**MS16-140**	**MS16-141**	**MS16-142**
Aggregate Severity Rating	**None**	**None**	**Critical**
Windows Vista Service Pack 2	Not applicable	Not applicable	Internet Explorer 9 (3197655) (Critical)
Windows Vista x64 Edition Service Pack 2	Not applicable	Not applicable	Internet Explorer 9 (3197655) (Critical)
Windows Server 2008			
Bulletin Identifier	**MS16-140**	**MS16-141**	**MS16-142**
Aggregate Severity Rating	**None**	**None**	**Critical**
Windows Server 2008 for 32-bit Systems Service Pack 2	Windows Server 2008 for 32-bit Systems Service Pack 2 (3193418)	Not applicable	Internet Explorer 9 (3197655) (Critical)
Windows Server 2008 for x64-based Systems Service Pack 2	Windows Server 2008 for x64-based Systems Service Pack 2 (3193418)	Not applicable	Internet Explorer 9 (3197655) (Critical)
Windows Server 2008 for Itanium-based Systems Service Pack 2	Windows Server 2008 for Itanium-based Systems Service Pack 2 (3193418)	Not applicable	Not applicable
Windows 7			
Bulletin Identifier	**MS16-140**	**MS16-141**	**MS16-142**
Aggregate Severity Rating	**None**	**None**	**Critical**
Windows 7 for 32-bit Systems Service Pack 1 Security Only	Not applicable	Not applicable	Internet Explorer 11 (3197867) (Critical)
Windows 7 for 32-bit Systems Service Pack 1 Monthly Roll Up	Not applicable	Not applicable	Internet Explorer 11 (3197868) (Critical)
Windows 7 for x64-based Systems Service Pack 1 Security Only	Not applicable	Not applicable	Internet Explorer 11 (3197867) (Critical)
Windows 7 for x64-based Systems Service Pack 1 Monthly Roll Up	Not applicable	Not applicable	Internet Explorer 11

			(3197868) (Critical)
Windows Server 2008 R2			
Bulletin Identifier	**MS16-140**	**MS16-141**	**MS16-142**
Aggregate Severity Rating	**None**	**None**	**Critical**
Windows Server 2008 R2 for x64-based Systems Service Pack 1 Security Only	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3197867) (Important)	Not applicable	Internet Explorer 11 (3197867) (Critical)
Windows Server 2008 R2 for x64-based Systems Service Pack 1 Monthly Roll Up	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3197868) (Important)	Not applicable	Internet Explorer 11 (3197868) (Critical)
Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 Security Only	Not applicable	Not applicable	Not applicable
Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 Monthly Rollup	Not applicable	Not applicable	Not applicable
Windows 8.1			
Bulletin Identifier	**MS16-140**	**MS16-141**	**MS16-142**
Aggregate Severity Rating	**Important**	**Critical**	**Critical**
Windows 8.1 for 32-bit Systems Security Only	Windows 8.1 for 32-bit Systems (3197873) (Important)	Adobe Flash Player (3202790) (Critical)	Internet Explorer 11 (3197873) (Critical)
Windows 8.1 for 32-bit Systems Monthly Roll Up	Windows 8.1 for 32-bit Systems (3197874) (Important)	Adobe Flash Player (3202790) (Critical)	Internet Explorer 11 (3197874) (Critical)
Windows 8.1 for x64-based Systems Security Only	Windows 8.1 for x64-based Systems (3197873) (Important)	Adobe Flash Player (3202790) (Critical)	Internet Explorer 11 (3197873) (Critical)
Windows 8.1 for x64-based Systems Monthly Roll Up	Windows 8.1 for x64-based Systems (3197874) (Important)	Adobe Flash Player (3202790) (Critical)	Internet Explorer 11 (3197874) (Critical)
Windows Server 2012 and Windows Server 2012 R2			
Bulletin Identifier	**MS16-140**	**MS16-141**	**MS16-142**
Aggregate Severity Rating	**Important**	**Moderate**	**Moderate**
Windows Server 2012 Security Only	Windows Server 2012 (3197876) (Important)	Adobe Flash Player (3202790) (Moderate)	Internet Explorer 10 (3197876) (Moderate)

Windows Server 2012 Monthly Roll Up	Windows Server 2012 (3197877) (Important)	Adobe Flash Player (3202790) (Moderate)	Internet Explorer 10 (3197877) (Moderate)
Windows Server 2012 R2 Security Only	Windows Server 2012 R2 (3197873) (Important)	Adobe Flash Player (3202790) (Moderate)	Internet Explorer 11 (3197873) (Moderate)
Windows Server 2012 R2 Monthly Roll Up	Windows Server 2012 R2 (3197874) (Important)	Adobe Flash Player (3202790) (Moderate)	Internet Explorer 11 (3197874) (Moderate)
Windows RT 8.1			
Bulletin Identifier	**MS16-140**	**MS16-141**	**MS16-142**
Aggregate Severity Rating	**Important**	**Important**	**None**
Windows RT 8.1 Monthly Roll Up	Windows RT 8.1 (3197874) (Important)	Adobe Flash Player (3202790) (Critical)	Not applicable
Windows 10			
Bulletin Identifier	**MS16-140**	**MS16-141**	**MS16-142**
Aggregate Severity Rating	**Important**	**Critical**	**Critical**
Windows 10 for 32-bit Systems	Windows 10 for 32-bit Systems (3198585) (Important)	Adobe Flash Player (3202790) (Critical)	Internet Explorer 11 (3198585) (Critical)
Windows 10 for x64-based Systems	Windows 10 for x64-based Systems (3198585) (Important)	Adobe Flash Player (3202790) (Critical)	Internet Explorer 11 (3198585) (Critical)
Windows 10 Version 1511 for 32-bit Systems	Windows 10 Version 1511 for 32-bit Systems (3198586) (Important)	Adobe Flash Player (3202790) (Critical)	Internet Explorer 11 (3198586) (Critical)
Windows 10 Version 1511 for x64-based Systems	Windows 10 Version 1511 for x64-based Systems (3198586) (Important)	Adobe Flash Player (3202790) (Critical)	Internet Explorer 11 (3198586) (Critical)
Windows 10 Version 1607 for 32-bit Systems	Windows 10 Version 1607 for 32-bit Systems (3200970) (Important)	Adobe Flash Player (3202790) (Critical)	Internet Explorer 11 (3200970) (Critical)
Windows 10 Version 1607 for x64-based Systems	Windows 10 Version 1607 for x64-based Systems (3200970) (Important)	Adobe Flash Player (3202790) (Critical)	Internet Explorer 11 (3200970) (Critical)
Windows Server 2016			

Bulletin Identifier	MS16-140	MS16-141	MS16-142
Aggregate Severity Rating	**Important**	**None**	**None**
Windows Server 2016 for x64-based Systems	Windows Server 2016 for x64-based Systems (3200970) (Important)	Not applicable	Not applicable
Server Core installation option			
Bulletin Identifier	**MS16-140**	**MS16-141**	**MS16-142**
Aggregate Severity Rating	**Important**	**None**	**None**
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (3190847) (Important)	Not applicable	Not applicable
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) (3190847) (Important)	Not applicable	Not applicable
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) Security Only	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3197867) (Important)	Not applicable	Not applicable
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) Monthly Rollup	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3197868) (Important)	Not applicable	Not applicable
Windows Server 2012 (Server Core installation) Security Only	Windows Server 2012 (Server Core installation) (3197876) (Important)	Not applicable	Not applicable
Windows Server 2012 (Server Core installation) Monthly Rollup	Windows Server 2012 (Server Core installation) (3197877) (Important)	Not applicable	Not applicable
Windows Server 2012 R2 (Server Core installation) Security Only	Windows Server 2012 R2 (Server Core installation) (3197873) (Important)	Not applicable	Not applicable
Windows Server 2012 R2 (Server Core installation) Monthly Rollup	Windows Server 2012 R2 (Server Core installation) (3197874) (Important)	Not applicable	Not applicable
Windows Server 2016 for x64-based Systems (Server Core installation)	Windows Server 2016 for x64-based Systems (Server Core installation) (3200970) (Critical)	Not applicable	Not applicable

Microsoft Office Suites and Software

Microsoft Office 2007	
Bulletin Identifier	**MS16-133**
Aggregate Severity Rating	**Important**
Microsoft Office 2007 Service Pack 3	Microsoft Excel 2007 Service Pack 3 (3118395) (Important) Microsoft Word 2007 (3127949) (Important) Microsoft Office 2007 Service Pack 3 (3118396) (Important) Microsoft Office 2007 Service Pack 3 (2986253) (Important)
Microsoft Office 2010	
Bulletin Identifier	**MS16-133**
Aggregate Severity Rating	**Important**
Microsoft Office 2010 Service Pack 2 (32-bit editions)	Microsoft Office 2010 Service Pack 2 (32-bit editions) (3127951) (Important) Microsoft Excel 2010 Service Pack 2 (32-bit editions) (3118390) (Important) Microsoft Word 2010 Service Pack 2 (32-bit editions) (3127953) (Important) Microsoft PowerPoint 2010 Service Pack 2 (32-bit editions) (3118378) (Important) Microsoft Office 2010 Service Pack 2 (32-bit editions) (3115120) (Important)
Microsoft Office 2010 Service Pack 2 (64-bit editions)	Microsoft Office 2010 Service Pack 2 (64-bit editions) (3127951) (Important) Microsoft Office 2010 Service Pack 2 (64-bit editions) (3127951) (Important) Microsoft Word 2010 Service Pack 2 (64-bit editions) (3127953) (Important) Microsoft PowerPoint 2010 Service Pack 2 (64-bit editions) (3118378) (Important) Microsoft Office 2010 Service Pack 2 (64-bit editions)

	(3115120) (Important)
Microsoft Office 2013	
Bulletin Identifier	**MS16-133**
Aggregate Severity Rating	**Important**
Microsoft Office 2013 Service Pack 1 (32-bit editions)	Microsoft Excel 2013 Service Pack 1 (32-bit editions) (3127921) (Important) Microsoft Office 2013 Service Pack 1 (32-bit editions) (3115153) (Important) Microsoft Word 2013 Service Pack 1 (32-bit editions) (3127932) (Important)
Microsoft Office 2013 Service Pack 1 (64-bit editions)	Microsoft Excel 2013 Service Pack 1 (64-bit editions) (3127921) (Important Microsoft Office 2013 Service Pack 1 (64-bit editions) (3115153) (Important) Microsoft Word 2013 Service Pack 1 (64-bit editions) (3127932) (Important)
Microsoft Office 2013 RT	
Bulletin Identifier	**MS16-133**
Aggregate Severity Rating	**Important**
Microsoft Office 2013 RT Service Pack 1	Microsoft Excel 2013 RT Service Pack 1 (3127921) (Important) Microsoft Office 2013 RT Service Pack 1 (3115153) (Important) Microsoft Word 2013 RT Service Pack 1 (3127932) (Important)
Microsoft Office 2016	
Bulletin Identifier	**MS16-133**
Aggregate Severity Rating	**Important**
Microsoft Office 2016 (32-bit edition)	Microsoft Excel 2016 (32-bit edition) (3127904) (Important) Microsoft Office 2016 (32-bit edition) (3115135) (Important)

Microsoft Office 2016 (64-bit edition)	Microsoft Excel 2016 (64-bit edition) (3127904) (Important) Microsoft Office 2016 (64-bit edition) (3115135) (Important)
Microsoft Office for Mac 2011	
Bulletin Identifier	**MS16-133**
Aggregate Severity Rating	**Important**
	Microsoft Excel for Mac 2011 (3198807) (Important) Microsoft Word for Mac 2011 (3198807) (Important)
Microsoft Office 2016 for Mac	
Bulletin Identifier	**MS16-133**
Aggregate Severity Rating	**Important**
	Microsoft Excel 2016 for Mac (3198798) (Important)
Other Office Software	
Bulletin Identifier	**MS16-133**
Aggregate Severity Rating	**Important**
Microsoft Office Compatibility Pack Service Pack 3	Microsoft Office Compatibility Pack Service Pack 3 (3127889) (Important) Microsoft Office Compatibility Pack Service Pack 3 (3127948 (Important)
Microsoft Excel Viewer	Microsoft Excel Viewer (3127893) (Important)
Microsoft PowerPoint Viewer	Microsoft PowerPoint Viewer (3118382) (Important)

Microsoft Office Services and Web Apps

Microsoft SharePoint Server 2010	
Bulletin Identifier	**MS16-133**

Aggregate Severity Rating	**Important**
Microsoft SharePoint Server 2010 Service Pack 2	Excel Services (3118381) (Important)
Microsoft SharePoint Server 2010 Service Pack 2	Word Automation Services (3127950) (Important)
Microsoft SharePoint Server 2013	
Bulletin Identifier	**MS16-133**
Aggregate Severity Rating	**Important**
Microsoft SharePoint Server 2013 Service Pack 1	Word Automation Services (3127927) (Important)
Microsoft Office Web Apps 2010	
Bulletin Identifier	**MS16-133**
Aggregate Severity Rating	**Important**
Microsoft Office Web Apps 2010 Service Pack 2	Microsoft Office Web Apps 2010 Service Pack 2 (3127954) (Important)
Microsoft Office Web Apps 2013	
Bulletin Identifier	**MS16-133**
Aggregate Severity Rating	**Important**
Microsoft Office Web Apps Server 2013 Service Pack 1	Microsoft Office Web Apps Server 2013 Service Pack 1 (3127929) (Important)

Microsoft SQL Server

SQL Server 2012 Service Pack 2	
Bulletin Identifier	**MS16-136**
Aggregate Severity Rating	**Important**
Microsoft SQL Server 2012 for x64-based Systems Service Pack 2	Microsoft SQL Server 2012 for x64-based Systems Service Pack 2 (GDR) (3194719) (Important) Microsoft SQL Server 2012 for x64-based Systems Service Pack 2 (3194725) (Important)
SQL Server 2012 Service Pack 3	
Bulletin Identifier	**MS16-136**

Aggregate Severity Rating	**Important**
Microsoft SQL Server 2012 for x64-based Systems Service Pack 3	Microsoft SQL Server 2012 for x64-based Systems Service Pack 3 (GDR) (3194721) (Important) Microsoft SQL Server 2012 for x64-based Systems Service Pack 3 (3194724) (Important)
SQL Server 2014 Service Pack 1	
Bulletin Identifier	**MS16-136**
Aggregate Severity Rating	**Important**
Microsoft SQL Server 2014 for x64-based Systems Service Pack 1	Microsoft SQL Server 2014 Service Pack 1 for x64-based Systems (GDR) (3194720) (Important) Microsoft SQL Server 2014 Service Pack 1 for x64-based Systems (3194722) (Important)
SQL Server 2014 Service Pack 2	
Bulletin Identifier	**MS16-136**
Aggregate Severity Rating	**Important**
Microsoft SQL Server 2014 for x64-based Systems Service Pack 2	Microsoft SQL Server 2014 Service Pack 2 for x64-based Systems (3194714) (Important) Microsoft SQL Server 2014 Service Pack 2 for x64-based Systems (3194718) (Important)
SQL Server 2016	
Bulletin Identifier	**MS16-136**
Aggregate Severity Rating	**Important**
Microsoft SQL Server 2016 for x64-based Systems	Microsoft SQL Server 2016 for x64-based Systems (GDR) (3194716) (Important) Microsoft SQL Server 2016 for x64-based Systems (3194717) (Important)

Detection and Deployment Tools and Guidance

Several resources are available to help administrators deploy security updates.

Microsoft Baseline Security Analyzer (MBSA) lets administrators scan local and remote systems for missing security updates and common security misconfigurations.

Windows Server Update Services (WSUS), Systems Management Server (SMS), and System Center Configuration Manager help administrators distribute security updates.

The Update Compatibility Evaluator components included with Application Compatibility Toolkit aid in streamlining the testing and validation of Windows updates against installed applications.

For information about these and other tools that are available, see Security Tools for IT Pros.

Acknowledgments

Microsoft recognizes the efforts of those in the security community who help us protect customers through responsible vulnerability disclosure. See Acknowledgments for more information.

Other Information

Microsoft Windows Malicious Software Removal Tool

For the bulletin release that occurs on the second Tuesday of each month, Microsoft has released an updated version of the Microsoft Windows Malicious Software Removal Tool on Windows Update, Microsoft Update, Windows Server Update Services, and the Download Center. No updated version of the Microsoft Windows Malicious Software Removal Tool is available for out-of-band security bulletin releases.

Non-Security Updates on MU, WU, and WSUS

For information about non-security releases on Windows Update and Microsoft Update, please see:

- Microsoft Knowledge Base Article 894199: Description of Software Update Services and Windows Server Update Services changes in content. Includes all Windows content.
- Updates from Past Months for Windows Server Update Services. Displays all new, revised, and rereleased updates for Microsoft products other than Microsoft Windows.

Microsoft Active Protections Program (MAPP)

To improve security protections for customers, Microsoft provides vulnerability information to major security software providers in advance of each monthly security update release. Security software providers can then use this vulnerability information to provide updated protections to customers via their security software or devices, such as antivirus, network-based intrusion detection systems, or host-based intrusion prevention systems. To determine whether active protections are available from security software providers, please visit the active protections websites provided by program partners listed in Microsoft Active Protections Program (MAPP) Partners.

Security Strategies and Community

Update Management Strategies

Security Guidance for Update Management provides additional information about Microsoft's best-practice recommendations for applying security updates.

Obtaining Other Security Updates

Updates for other security issues are available from the following locations:

- Security updates are available from Microsoft Download Center. You can find them most easily by doing a keyword search for "security update".
- Updates for consumer platforms are available from Microsoft Update.

IT Pro Security Community

Learn to improve security and optimize your IT infrastructure, and participate with other IT Pros on security topics in IT Pro Security Community.

Support

The affected software listed has been tested to determine which versions are affected. Other versions are past their support life cycle. To determine the support life cycle for your software version, visit Microsoft Support Lifecycle.

Security solutions for IT professionals: TechNet Security Troubleshooting and Support

Help protect your computer that is running Windows from viruses and malware: Virus Solution and Security Center

Local support according to your country: International Support

Disclaimer

Revisions

- V1.0 (November 8, 2016): Bulletin Summary published.
  V1.1 (November 23, 2016) Revised bulletin to announce a detection change for certain servers running Windows Servers 2012, Windows Server 2012 R2, and Windows Server 2016. Affected servers will not automatically receive the security update. For more information about the servers affected by this detection change, see Knowledge Base Article 3193479.

Page generated 2017-04-14 09:10-07:00.