Microsoft Security Bulletin Summary for December 2016

Published: December 13, 2016 | Updated: December 21, 2016

Version: 1.2

This bulletin summary lists security bulletins released for December 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**.

Note As a reminder, the Security Updates Guide will be replacing security bulletins as of February 2017. Please see our blog post, Furthering our commitment to security updates, for more details.

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
MS16-144	**Cumulative Security Update for Internet Explorer (3204059)** 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	---------	Microsoft Windows, Internet Explorer
MS16-145	**Cumulative Security Update for Microsoft Edge (3204062)** 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	Critical Remote Code Execution	Requires restart	---------	Microsoft Windows, Microsoft Edge

	impacted than users with administrative user rights.				
MS16-146	**Security Update for Microsoft Graphics Component (3204066)** This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow remote code execution if a user either visits a specially crafted website or opens a specially crafted document. 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.	Critical Remote Code Execution	Requires restart	---------	Microsoft Windows
MS16-147	**Security Update for Microsoft Uniscribe (3204063)** This security update resolves a vulnerability in Windows Uniscribe. The vulnerability could allow remote code execution if a user visits a specially crafted website or opens a specially crafted document. 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.	Critical Remote Code Execution	Requires restart	---------	Microsoft Windows
MS16-148	**Security Update for Microsoft Office (3204068)** 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.	Critical Remote Code Execution	May require restart	---------	Microsoft Office, Microsoft Office Services and Web Apps
MS16-149	**Security Update for Microsoft Windows (3205655)** This security update resolves vulnerabilities in Microsoft Windows. The more severe of the vulnerabilities could allow elevation of privilege if a locally authenticated attacker runs a specially crafted application.	Important Elevation of Privilege	Requires restart	---------	Microsoft Windows
MS16-150	**Security Update for Secure Kernel Mode (3205642)** This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if a locally-authenticated attacker runs a specially crafted application on a targeted system. An attacker who successfully exploited the vulnerability could violate virtual trust levels (VTL).	Important Elevation of Privilege	Requires restart	---------	Microsoft Windows
MS16-151	**Security Update for Windows Kernel-Mode Drivers (3205651)** This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities	Important Elevation of Privilege	Requires restart	---------	Microsoft Windows

	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.				
MS16-152	**Security Update for Windows Kernel (3199709)** This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow information disclosure when the Windows kernel improperly handles objects in memory.	Important Information Disclosure	Requires restart	---------	Microsoft Windows
MS16-153	**Security Update for Common Log File System Driver (3207328)** This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow information disclosure when the Windows Common Log File System (CLFS) driver improperly handles objects in memory. In a local attack scenario, an attacker could exploit this vulnerability by running a specially crafted application to bypass security measures on the affected system allowing further exploitation.	Important Information Disclosure	Requires restart	---------	Microsoft Windows
MS16-154	**Security Update for Adobe Flash Player (3209498)** 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
MS16-155	**Security Update for .NET Framework (3205640)** This security update resolves a vulnerability in Microsoft .NET 4.6.2 Framework's Data Provider for SQL Server. A security vulnerability exists in Microsoft .NET Framework 4.6.2 that could allow an attacker to access information that is defended by the Always Encrypted feature.	Important Information Disclosure	Requires restart	3210137 3210138	Microsoft Windows, Microsoft .NET Framework

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	Exploitability Assessment for	Denial of Service

		Latest Software Release	Older Software Release	Exploitability Assessment
MS16-144: Cumulative Security Update for Internet Explorer (3204059)				
CVE-2016-7202	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-7278	Windows Hyperlink Object Library Information Disclosure Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2016-7279	Microsoft Browser Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-7281	Microsoft Browser Security Feature Bypass	3 - Exploitation Unlikely	3 - Exploitation Unlikely	Not applicable
CVE-2016-7282	Microsoft Browser Information Disclosure Vulnerability	3 - Exploitation Unlikely	3 - Exploitation Unlikely	Not applicable
CVE-2016-7283	Internet Explorer Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-7284	Internet Explorer Information Disclosure Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2016-7287	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
MS16-145: Cumulative Security Update for Microsoft Edge (3204062)				
CVE-2016-7181	Microsoft Edge Memory Corruption Vulnerability	3 - Exploitation Unlikely	4 - Not affected	Not applicable
CVE-2016-7206	Microsoft Edge Information Disclosure Vulnerability	3 - Exploitation Unlikely	4 - Not affected	Not applicable
CVE-2016-7279	Microsoft Browser Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Permanent
CVE-2016-7280	Microsoft Edge Information	3 - Exploitation Unlikely	4 - Not affected	Not applicable

	Disclosure Vulnerability			
CVE-2016-7281	Microsoft Browser Security Feature Bypass	3 - Exploitation Unlikely	4 - Not affected	Not applicable
CVE-2016-7282	Microsoft Browser Information Disclosure Vulnerability	3 - Exploitation Unlikely	4 - Not affected	Not applicable
CVE-2016-7286	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-7287	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-7288	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-7296	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-7297	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
MS16-146: Security Update for Microsoft Graphics Component (3204066)				
CVE-2016-7257	GDI Information Disclosure Vulnerability	4 - Not affected	2 - Exploitation Less Likely	Not applicable
CVE-2016-7272	Windows Graphics Remote Code Execution Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-7273	Windows Graphics Remote Code Execution Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
MS16-147: Security Update for Microsoft Uniscribe (3204063)				
CVE-2016-7274	Windows Uniscribe Remote Code Execution Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
MS16-148: Security Update for Microsoft Office (3204068)				
CVE-2016-7257	GDI Information Disclosure Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable

CVE-2016-7262	Microsoft Office Security Feature Bypass Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-7263	Microsoft Office Memory Corruption Vulnerability	3 - Exploitation Unlikely	3 - Exploitation Unlikely	Not applicable
CVE-2016-7264	Microsoft Office Information Disclosure Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2016-7265	Microsoft Office Information Disclosure Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2016-7266	Microsoft Office Security Feature Bypass Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-7267	Microsoft Office Security Feature Bypass Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-7268	Microsoft Office Information Disclosure Vulnerability	4 - Not affected	2 - Exploitation Less Likely	Not applicable
CVE-2016-7274	Windows Uniscribe Remote Code Execution Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-7275	Microsoft Office OLE DLL Side Loading Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-7276	Microsoft Office Information Disclosure Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2016-7277	Microsoft Office Memory Corruption Vulnerability	2 - Exploitation Less Likely	4 - Not affected	Not applicable
CVE-2016-7289	Microsoft Office Memory Corruption Vulnerability	4 - Not affected	1 - Exploitation More Likely	Not applicable
CVE-2016-7290	Microsoft Office Information Disclosure Vulnerability	4 - Not affected	3 - Exploitation Unlikely	Not applicable

CVE-2016-7291	Microsoft Office Information Disclosure Vulnerability	4 - Not affected	3 - Exploitation Unlikely	Not applicable
CVE-2016-7300	Microsoft Office Elevation of Privilege Vulnerability	3 - Exploitation Unlikely	3 - Exploitation Unlikely	Not applicable
MS16-149: Security Update for Microsoft Windows (3205655)				
CVE-2016-7219	Windows Crypto Driver Information Disclosure Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-7292	Windows Installer Elevation of Privilege Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
MS16-150: Security Update for Secure Kernel Mode (3205642)				
CVE-2016-7271	Secure Kernel Mode Elevation of Privilege Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
MS16-151: Security Update for Windows Kernel-Mode Drivers (3205651)				
CVE-2016-7259	Win32k Elevation of Privilege Vulnerability	3 - Exploitation Unlikely	2 - Exploitation Less Likely	Permanent
CVE-2016-7260	Win32k Elevation of Privilege Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
MS16-152: Security Update for Windows Kernel (3199709)				
CVE-2016-7258	Windows Kernel Memory Address Information Disclosure Vulnerability	3 - Exploitation Unlikely	3 - Exploitation Unlikely	Not applicable
MS16-153: Security Update for Common Log File System Driver (3207328)				
CVE-2016-7295	Windows Common Log File System Driver Information Disclosure Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
MS16-154: Security Update for Adobe Flash Player (3202790)				
APSB16-39	See Adobe Security Bulletin APSB16-39 for vulnerability severity and	---	---	Not applicable

	update priority ratings.			
MS16-155: Security Update for .NET Framework (3205640)				
CVE-2016-7270	.NET Framework Information Disclosure Vulnerability	3 - Exploitation Unlikely	4 - Not affected	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 2)

Windows Vista					
Bulletin Identifier	**MS16-144**	**MS16-145**	**MS16-146**	**MS16-147**	**MS16-149**
Aggregate Severity Rating	**Critical**	**None**	**Critical**	**Critical**	**Important**
Windows Vista Service Pack 2	Internet Explorer 9 (3203621) (Critical) Microsoft Windows Hyperlink Object Library (3208481) (Critical)	Not applicable	Windows Vista Service Pack 2 (3204724) (Important) Windows Vista Service Pack 2 (3205638) (Critical)	Windows Vista Service Pack 2 (3196348) (Critical)	Windows Vista Service Pack 2 (3204808) (Important) Windows Vista Service Pack 2 (3196726) (Important)
Windows Vista x64 Edition Service Pack 2	Internet Explorer 9 (3203621) (Critical) Microsoft Windows Hyperlink Object Library (3208481) (Critical)	Not applicable	Windows Vista x64 Edition Service Pack 2 (3204724) (Important) Windows Vista x64 Edition Service Pack 2 (3205638) (Critical)	Windows Vista x64 Edition Service Pack 2 (3196348) (Critical)	Windows Vista x64 Edition Service Pack 2 (3204808) (Important) Windows Vista x64 Edition Service Pack 2 (3196726) (Important)
Windows Server 2008					
Bulletin Identifier	**MS16-144**	**MS16-145**	**MS16-146**	**MS16-147**	**MS16-149**
Aggregate Severity Rating	**Moderate**	**None**	**Critical**	**Critical**	**Important**
Windows Server 2008 for	Internet	Not applicable	Windows Server	Windows Server	Windows Server

32-bit Systems Service Pack 2	Explorer 9 (3203621) (Moderate) Microsoft Windows Hyperlink Object Library (3208481) (Moderate)		2008 for 32-bit Systems Service Pack 2 (3204724) (Important) Windows Server 2008 for 32-bit Systems Service Pack 2 (3205638) (Critical)	2008 for 32-bit Systems Service Pack 2 (3196348) (Critical)	2008 for 32-bit Systems Service Pack 2 (3204808) (Important) Windows Server 2008 for 32-bit Systems Service Pack 2 (3196726) (Important)
Windows Server 2008 for x64-based Systems Service Pack 2	Internet Explorer 9 (3203621) (Moderate) Microsoft Windows Hyperlink Object Library (3208481) (Moderate)	Not applicable	Windows Server 2008 for x64-based Systems Service Pack 2 (3204724) (Important) Windows Server 2008 for x64-based Systems Service Pack 2 (3205638) (Critical)	Windows Server 2008 for x64-based Systems Service Pack 2 (3196348) (Critical)	Windows Server 2008 for x64-based Systems Service Pack 2 (3204808) (Important) Windows Server 2008 for x64-based Systems Service Pack 2 (3196726) (Important)
Windows Server 2008 for Itanium-based Systems Service Pack 2	Not applicable	Not applicable	Windows Server 2008 for Itanium-based Systems Service Pack 2 (3204724) (Important) Windows Server 2008 for Itanium-based Systems Service Pack 2 (3205638) (Critical)	Windows Server 2008 for Itanium-based Systems Service Pack 2 (3196348) (Critical)	Windows Server 2008 for Itanium-based Systems Service Pack 2 (3204808) (Important) Windows Server 2008 for Itanium-based Systems Service Pack 2 (3196726) (Important)
Windows 7					
Bulletin Identifier	**MS16-144**	**MS16-145**	**MS16-146**	**MS16-147**	**MS16-149**
Aggregate Severity Rating	**Critical**	**None**	**Critical**	**Critical**	**Important**
Windows 7 for 32-bit Systems Service Pack 1 Security Only	Internet Explorer 11 (3205394) (Critical)	Not applicable	Windows 7 for 32-bit Systems Service Pack 1 (3205394) (Critical)	Windows 7 for 32-bit Systems Service Pack 1 (3205394) (Critical)	Windows 7 for 32-bit Systems Service Pack 1 (3205394) (Important)
Windows 7 for 32-bit Systems Service Pack 1 Monthly Rollup	Internet Explorer 11 (3207752) (Critical)	Not applicable	Windows 7 for 32-bit Systems Service Pack 1 (3207752) (Critical)	Windows 7 for 32-bit Systems Service Pack 1 (3207752) (Critical)	Windows 7 for 32-bit Systems Service Pack 1 (3207752) (Important)
Windows 7 for x64-based Systems Service Pack 1 Security Only	Internet Explorer 11 (3205394) (Critical)	Not applicable	Windows 7 for x64-based Systems Service Pack 1 (3205394) (Critical)	Windows 7 for x64-based Systems Service Pack 1 (3205394) (Critical)	Windows 7 for x64-based Systems Service Pack 1 (3205394) (Important)

Windows 7 for x64-based Systems Service Pack 1 Monthly Rollup	Internet Explorer 11 (3207752) (Critical)	Not applicable	Windows 7 for x64-based Systems Service Pack 1 (3207752) (Critical)	Windows 7 for x64-based Systems Service Pack 1 (3207752) (Critical)	Windows 7 for x64-based Systems Service Pack 1 (3207752) (Important)
Windows Server 2008 R2					
Bulletin Identifier	**MS16-144**	**MS16-145**	**MS16-146**	**MS16-147**	**MS16-149**
Aggregate Severity Rating	**Moderate**	**None**	**Critical**	**Critical**	**Important**
Windows Server 2008 R2 for x64-based Systems Service Pack 1 Security Only	Internet Explorer 11 (3205394) (Moderate)	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3205394) (Critical)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3205394) (Critical)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3205394) (Important)
Windows Server 2008 R2 for x64-based Systems Service Pack 1 Monthly Rollup	Internet Explorer 11 (3207752) (Moderate)	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3207752) (Critical)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3207752) (Critical)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3207752) (Important)
Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 Security Only	Not applicable	Not applicable	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3205394) (Critical)	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3205394) (Critical)	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3205394) (Important)
Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 Monthly Rollup	Not applicable	Not applicable	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3207752) (Critical)	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3207752) (Critical)	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3207752) (Important)
Windows 8.1					
Bulletin Identifier	**MS16-144**	**MS16-145**	**MS16-146**	**MS16-147**	**MS16-149**
Aggregate Severity Rating	**Critical**	**None**	**Critical**	**Critical**	**Important**
Windows 8.1 for 32-bit Systems Security Only	Internet Explorer 11 (3205400) (Critical)	Not applicable	Windows 8.1 for 32-bit Systems (3205400) (Critical)	Windows 8.1 for 32-bit Systems (3205400) (Critical)	Windows 8.1 for 32-bit Systems (3205400) (Important)
Windows 8.1 for 32-bit Systems Monthly Rollup	Internet Explorer 11 (3205401) (Critical)	Not applicable	Windows 8.1 for 32-bit Systems (3205401) (Critical)	Windows 8.1 for 32-bit Systems (3205401) (Critical)	Windows 8.1 for 32-bit Systems (3205401) (Important)
Windows 8.1 for x64-based Systems Security Only	Internet Explorer 11	Not applicable	Windows 8.1 for x64-based Systems	Windows 8.1 for x64-based Systems	Windows 8.1 for x64-based Systems

	(3205400) (Critical)		(3205400) (Critical)	(3205400) (Critical)	(3205400) (Important)
Windows 8.1 for x64-based Systems Monthly Rollup	Internet Explorer 11 (3205401) (Critical)	Not applicable	Windows 8.1 for x64-based Systems (3205401) (Critical)	Windows 8.1 for x64-based Systems (3205401) (Critical)	Windows 8.1 for x64-based Systems (3205401) (Important)
Windows Server 2012 and Windows Server 2012 R2					
Bulletin Identifier	**MS16-144**	**MS16-145**	**MS16-146**	**MS16-147**	**MS16-149**
Aggregate Severity Rating	**Moderate**	**None**	**Critical**	**Critical**	**Important**
Windows Server 2012 Security Only	Internet Explorer 10 (3205408) (Moderate)	Not applicable	Windows Server 2012 (3205408) (Critical)	Windows Server 2012 (3205408) (Critical)	Windows Server 2012 (3205408) (Important)
Windows Server 2012 Monthly Rollup	Internet Explorer 10 (3205409) (Moderate)	Not applicable	Windows Server 2012 (3205409) (Critical)	Windows Server 2012 (3205409) (Critical)	Windows Server 2012 (3205409) (Important)
Windows Server 2012 R2 Security Only	Internet Explorer 11 (3205400) (Moderate)	Not applicable	Windows Server 2012 R2 (3205400) (Critical)	Windows Server 2012 R2 (3205400) (Critical)	Windows Server 2012 R2 (3205400) (Important)
Windows Server 2012 R2 Monthly Rollup	Internet Explorer 11 (3205401) (Moderate)	Not applicable	Windows Server 2012 R2 (3205401) (Critical)	Windows Server 2012 R2 (3205401) (Critical)	Windows Server 2012 R2 (3205401) (Important)
Windows RT 8.1					
Bulletin Identifier	**MS16-144**	**MS16-145**	**MS16-146**	**MS16-147**	**MS16-149**
Aggregate Severity Rating	**Critical**	**None**	**Critical**	**Critical**	**Important**
Windows RT 8.1 Monthly Rollup	Internet Explorer 11 (3205401) (Critical)	Not applicable	Windows RT 8.1 (3205401) (Critical)	Windows RT 8.1 (3205401) (Critical)	Windows RT 8.1 (3205401) (Important)
Windows 10					
Bulletin Identifier	**MS16-144**	**MS16-145**	**MS16-146**	**MS16-147**	**MS16-149**
Aggregate Severity Rating	**Critical**	**Critical**	**Critical**	**Critical**	**Important**
Windows 10 for 32-bit Systems	Internet Explorer 11 (3205383) (Critical)	Microsoft Edge (3205383) (Critical)	Windows 10 for 32-bit Systems (3205383) (Critical)	Windows 10 for 32-bit Systems (3205383) (Critical)	Windows 10 for 32-bit Systems (3205383) (Important)
Windows 10 for x64-based Systems	Internet Explorer 11 (3205383) (Critical)	Microsoft Edge (3205383) (Critical)	Windows 10 for x64-based Systems	Windows 10 for x64-based Systems	Windows 10 for x64-based Systems (3205383) (Important)

			(3205383) (Critical)	(3205383) (Critical)	
Windows 10 Version 1511 for 32-bit Systems	Internet Explorer 11 (3205386) (Critical)	Microsoft Edge (3205386) (Critical)	Windows 10 Version 1511 for 32-bit Systems (3205386) (Critical)	Windows 10 Version 1511 for 32-bit Systems (3205386) (Critical)	Windows 10 Version 1511 for 32-bit Systems (3205386) (Important)
Windows 10 Version 1511 for x64-based Systems	Internet Explorer 11 (3205386) (Critical)	Microsoft Edge (3205386) (Critical)	Windows 10 Version 1511 for x64-based Systems (3205386) (Critical)	Windows 10 Version 1511 for x64-based Systems (3205386) (Critical)	Windows 10 Version 1511 for x64-based Systems (3205386) (Important)
Windows 10 Version 1607 for 32-bit Systems	Internet Explorer 11 (3206632) (Critical)	Microsoft Edge (3206632) (Critical)	Windows 10 Version 1607 for 32-bit Systems (3206632) (Critical)	Windows 10 Version 1607 for 32-bit Systems (3206632) (Critical)	Windows 10 Version 1607 for 32-bit Systems (3206632) (Important)
Windows 10 Version 1607 for x64-based Systems	Internet Explorer 11 (3206632) (Critical)	Microsoft Edge (3206632) (Critical)	Windows 10 Version 1607 for x64-based Systems (3206632) (Critical)	Windows 10 Version 1607 for x64-based Systems (3206632) (Critical)	Windows 10 Version 1607 for x64-based Systems (3206632) (Important)
Windows Server 2016					
Bulletin Identifier	**MS16-144**	**MS16-145**	**MS16-146**	**MS16-147**	**MS16-149**
Aggregate Severity Rating	**Moderate**	**Moderate**	**Critical**	**Critical**	**Important**
Windows Server 2016 for x64-based Systems	Internet Explorer 11 (3206632) (Moderate)	Microsoft Edge (3206632) (Moderate)	Windows Server 2016 for x64-based Systems (3206632) (Critical)	Windows Server 2016 for x64-based Systems (3206632) (Critical)	Windows Server 2016 for x64-based Systems (3206632) (Important)
Server Core installation option					
Bulletin Identifier	**MS16-144**	**MS16-145**	**MS16-146**	**MS16-147**	**MS16-149**
Aggregate Severity Rating	**None**	**None**	**Critical**	**Critical**	**Important**
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	Not applicable	Not applicable	Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (3204724) (Important) Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (3205638) (Critical)	Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (3196348) (Critical)	Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (3204808) (Important) Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (3196726) (Important)

Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	Not applicable	Not applicable	Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) (3204724) (Important) Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) (3205638) (Critical)	Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) (3196348) (Critical)	Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) (3204808) (Important) Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) (3196726) (Important)
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) Security Only	Not applicable	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3205394) (Critical)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3205394) (Critical)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3205394) (Important)
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) Monthly Rollup	Not applicable	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3207752) (Critical)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3207752) (Critical)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3207752) (Important)
Windows Server 2012 (Server Core installation) Security Only	Not applicable	Not applicable	Windows Server 2012 (Server Core installation) (3205408) (Critical)	Windows Server 2012 (Server Core installation) (3205408) (Critical)	Windows Server 2012 (Server Core installation) (3205408) (Important)
Windows Server 2012 (Server Core installation) Monthly Rollup	Not applicable	Not applicable	Windows Server 2012 (Server Core installation) (3205409) (Critical)	Windows Server 2012 (Server Core installation) (3205409) (Critical)	Windows Server 2012 (Server Core installation) (3205409) (Important)
Windows Server 2012 R2 (Server Core installation) Security Only	Not applicable	Not applicable	Windows Server 2012 R2 (Server Core installation) (3205400) (Critical)	Windows Server 2012 R2 (Server Core installation) (3205400) (Critical)	Windows Server 2012 R2 (Server Core installation) (3205400) (Important)
Windows Server 2012 R2 (Server Core installation) Monthly Rollup	Not applicable	Not applicable	Windows Server 2012 R2 (Server Core installation) (3205401) (Critical)	Windows Server 2012 R2 (Server Core installation) (3205401) (Critical)	Windows Server 2012 R2 (Server Core installation) (3205401) (Important)
Windows Server 2016 for x64-based Systems (Server Core installation)	Not applicable	Not applicable	Windows Server 2016 for x64-based Systems (Server Core installation)	Windows Server 2016 for x64-based Systems (Server Core installation)	Windows Server 2016 for x64-based Systems (Server Core installation)

			(3206632) (Critical)	(3206632) (Critical)	(3206632) (Important)

Windows Operating Systems and Components (Table 2 of 2)

Windows Vista					
Bulletin Identifier	**MS16-150**	**MS16-151**	**MS16-152**	**MS16-153**	**MS16-154**
Aggregate Severity Rating	**None**	**Important**	**None**	**Important**	**None**
Windows Vista Service Pack 2	Not applicable	Windows Vista Service Pack 2 (3204723) (Important)	Not applicable	Windows Vista Service Pack 2 (3203838) (Important)	Not applicable
Windows Vista x64 Edition Service Pack 2	Not applicable	Windows Vista x64 Edition Service Pack 2 (3204723) (Important)	Not applicable	Windows Vista x64 Edition Service Pack 2 (3203838) (Important)	Not applicable
Windows Server 2008					
Bulletin Identifier	**MS16-150**	**MS16-151**	**MS16-152**	**MS16-153**	**MS16-154**
Aggregate Severity Rating	**None**	**Important**	**None**	**Important**	**None**
Windows Server 2008 for 32-bit Systems Service Pack 2	Not applicable	Windows Server 2008 for 32-bit Systems Service Pack 2 (3204723) (Important)	Not applicable	Windows Server 2008 for 32-bit Systems Service Pack 2 (3203838) (Important)	Not applicable
Windows Server 2008 for x64-based Systems Service Pack 2	Not applicable	Windows Server 2008 for x64-based Systems Service Pack 2 (3204723) (Important)	Not applicable	Windows Server 2008 for x64-based Systems Service Pack 2 (3203838) (Important)	Not applicable
Windows Server 2008 for Itanium-based Systems Service Pack 2	Not applicable	Windows Server 2008 for Itanium-based Systems Service Pack 2 (3204723) (Important)	Not applicable	Windows Server 2008 for Itanium-based Systems Service Pack 2 (3203838) (Important)	Not applicable
Windows 7					
Bulletin Identifier	**MS16-150**	**MS16-151**	**MS16-152**	**MS16-153**	**MS16-154**
Aggregate Severity Rating	**None**	**Important**	**None**	**Important**	**None**
Windows 7 for 32-bit Systems Service Pack 1 Security Only	Not applicable	Windows 7 for 32-bit Systems Service Pack 1 (3205394) (Important)	Not applicable	Windows 7 for 32-bit Systems Service Pack 1	Not applicable

				(3205394) (Important)	
Windows 7 for 32-bit Systems Service Pack 1 Monthly Rollup	Not applicable	Windows 7 for 32-bit Systems Service Pack 1 (3207752) (Important)	Not applicable	Windows 7 for 32-bit Systems Service Pack 1 (3207752) (Important)	Not applicable
Windows 7 for x64-based Systems Service Pack 1 Security Only	Not applicable	Windows 7 for x64-based Systems Service Pack 1 (3205394) (Important)	Not applicable	Windows 7 for x64-based Systems Service Pack 1 (3205394) (Important)	Not applicable
Windows 7 for x64-based Systems Service Pack 1 Monthly Rollup	Not applicable	Windows 7 for x64-based Systems Service Pack 1 (3207752) (Important)	Not applicable	Windows 7 for x64-based Systems Service Pack 1 (3207752) (Important)	Not applicable
Windows Server 2008 R2					
Bulletin Identifier	**MS16-150**	**MS16-151**	**MS16-152**	**MS16-153**	**MS16-154**
Aggregate Severity Rating	**None**	**Important**	**None**	**Important**	**None**
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 (3205394) (Important)	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3205394) (Important)	Not applicable
Windows Server 2008 R2 for x64-based Systems Service Pack 1 Monthly Rollup	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3207752) (Important)	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3207752) (Important)	Not applicable
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 (3205394) (Important)	Not applicable	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3205394) (Important)	Not applicable
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 (3207752) (Important)	Not applicable	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3207752) (Important)	Not applicable
Windows 8.1					
Bulletin Identifier	**MS16-150**	**MS16-151**	**MS16-152**	**MS16-153**	**MS16-154**
Aggregate Severity Rating	**None**	**Important**	**None**	**Important**	**Critcal**

Windows 8.1 for 32-bit Systems Security Only	Not applicable	Windows 8.1 for 32-bit Systems (3205400) (Important)	Not applicable	Windows 8.1 for 32-bit Systems (3205400) (Important)	Adobe Flash Player (3209498) (Critical)
Windows 8.1 for 32-bit Systems Monthly Rollup	Not applicable	Windows 8.1 for 32-bit Systems (3205401) (Important)	Not applicable	Windows 8.1 for 32-bit Systems (3205401) (Important)	Not applicable
Windows 8.1 for x64-based Systems Security Only	Not applicable	Windows 8.1 for x64-based Systems (3205400) (Important)	Not applicable	Windows 8.1 for x64-based Systems (3205400) (Important)	Adobe Flash Player (3209498) (Critical)
Windows 8.1 for x64-based Systems Monthly Rollup	Not applicable	Windows 8.1 for x64-based Systems (3205401) (Important)	Not applicable	Windows 8.1 for x64-based Systems (3205401) (Important)	Not applicable
Windows Server 2012 and Windows Server 2012 R2					
Bulletin Identifier	**MS16-150**	**MS16-151**	**MS16-152**	**MS16-153**	**MS16-154**
Aggregate Severity Rating	**None**	**Important**	**None**	**Important**	**Moderate**
Windows Server 2012 Security Only	Not applicable	Windows Server 2012 (3205408) (Important)	Not applicable	Windows Server 2012 (3205408) (Important)	Adobe Flash Player (3209498) (Moderate)
Windows Server 2012 Monthly Rollup	Not applicable	Windows Server 2012 (3205409) (Important)	Not applicable	Windows Server 2012 (3205409) (Important)	Not applicable
Windows Server 2012 R2 Security Only	Not applicable	Windows Server 2012 R2 (3205400) (Important)	Not applicable	Windows Server 2012 R2 (3205400) (Important)	Adobe Flash Player (3209498) (Moderate)
Windows Server 2012 R2 Monthly Rollup	Not applicable	Windows Server 2012 R2 (3205401) (Important)	Not applicable	Windows Server 2012 R2 (3205401) (Important)	Not applicable
Windows RT 8.1					
Bulletin Identifier	**MS16-150**	**MS16-151**	**MS16-152**	**MS16-153**	**MS16-154**
Aggregate Severity Rating	**None**	**Important**	**None**	**Important**	**Critical**
Windows RT 8.1 Monthly Rollup	Not applicable	Windows RT 8.1 (3205401) (Important)	Not applicable	Windows RT 8.1 (3205401) (Important)	Adobe Flash Player (3209498) (Critical)
Windows 10					
Bulletin Identifier	**MS16-150**	**MS16-151**	**MS16-152**	**MS16-153**	**MS16-154**
Aggregate Severity	**Important**	**Important**	**Important**	**Important**	**Critical**

Rating					
Windows 10 for 32-bit Systems	Windows 10 for 32-bit Systems (3205383) (Important)	Windows 10 for 32-bit Systems (3205383) (Important)	Windows 10 for 32-bit Systems (3205383) (Important)	Windows 10 for 32-bit Systems (3205383) (Important)	Adobe Flash Player (3209498) (Critical)
Windows 10 for x64-based Systems	Windows 10 for x64-based Systems (3205383) (Important)	Windows 10 for x64-based Systems (3205383) (Important)	Windows 10 for x64-based Systems (3205383) (Important)	Windows 10 for x64-based Systems (3205383) (Important)	Adobe Flash Player (3209498) (Critical)
Windows 10 Version 1511 for 32-bit Systems	Windows 10 Version 1511 for 32-bit Systems (3205386) (Important)	Windows 10 Version 1511 for 32-bit Systems (3205386) (Important)	Windows 10 Version 1511 for 32-bit Systems (3205386) (Important)	Windows 10 Version 1511 for 32-bit Systems (3205386) (Important)	Adobe Flash Player (3209498) (Critical)
Windows 10 Version 1511 for x64-based Systems	Windows 10 Version 1511 for x64-based Systems (3205386) (Important)	Windows 10 Version 1511 for x64-based Systems (3205386) (Important)	Windows 10 Version 1511 for x64-based Systems (3205386) (Important)	Windows 10 Version 1511 for x64-based Systems (3205386) (Important)	Adobe Flash Player (3209498) (Critical)
Windows 10 Version 1607 for 32-bit Systems	Windows 10 Version 1607 for 32-bit Systems (3206632) (Important)	Windows 10 Version 1607 for 32-bit Systems (3206632) (Important)	Windows 10 Version 1607 for 32-bit Systems (3206632) (Important)	Windows 10 Version 1607 for 32-bit Systems (3206632) (Important)	Adobe Flash Player (3209498) (Critical)
Windows 10 Version 1607 for x64-based Systems	Windows 10 Version 1607 for x64-based Systems (3206632) (Important)	Windows 10 Version 1607 for x64-based Systems (3206632) (Important)	Windows 10 Version 1607 for x64-based Systems (3206632) (Important)	Windows 10 Version 1607 for x64-based Systems (3206632) (Important)	Adobe Flash Player (3209498) (Critical)
Windows Server 2016					
Bulletin Identifier	**MS16-150**	**MS16-151**	**MS16-152**	**MS16-153**	**MS16-154**
Aggregate Severity Rating	**Important**	**Important**	**Important**	**Important**	**Moderate**
Windows Server 2016 for x64-based Systems	Windows Server 2016 for x64-based Systems (3206632) (Important)	Windows Server 2016 for x64-based Systems (3206632) (Important)	Windows Server 2016 for x64-based Systems (3206632) (Important)	Windows Server 2016 for x64-based Systems (3206632) (Important)	Adobe Flash Player (3209498) (Moderate)
Server Core installation					
Bulletin Identifier	**MS16-150**	**MS16-151**	**MS16-152**	**MS16-153**	**MS16-154**
Aggregate Severity Rating	**Important**	**Important**	**Important**	**Important**	**None**
Windows Server 2008 for 32-bit Systems	Not applicable	Windows Server 2008 for 32-bit Systems	Not applicable	Windows Server 2008 for 32-bit	Not applicable

Service Pack 2 (Server Core installation)		Service Pack 2 (Server Core installation) (3204723) (Important)		Systems Service Pack 2 (Server Core installation) (3203838) (Important)	
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	Not applicable	Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) (3204723) (Important)	Not applicable	Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) (3203838) (Important)	Not applicable
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) (3205394) (Important)	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3205394) (Important)	Not applicable
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) (3207752) (Important)	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3207752) (Important)	Not applicable
Windows Server 2012 (Server Core installation) Security Only	Not applicable	Windows Server 2012 (Server Core installation) (3205408) (Important)	Not applicable	Not applicable	Not applicable
Windows Server 2012 (Server Core installation) Monthly Rollup	Not applicable	Windows Server 2012 (Server Core installation) (3205409) (Important)	Not applicable	Not applicable	Not applicable
Windows Server 2012 R2 (Server Core installation) Security Only	Not applicable	Windows Server 2012 R2 (Server Core installation) (3205400) (Important)	Not applicable	Windows Server 2012 R2 (Server Core installation) (3205400) (Important)	Not applicable
Windows Server 2012 R2 (Server Core installation) Monthly Rollup	Not applicable	Windows Server 2012 R2 (Server Core installation) (3205401) (Important)	Not applicable	Windows Server 2012 R2 (Server Core installation) (3205401) (Important)	Not applicable
Windows Server 2016 for x64-based Systems (Server Core installation)	Windows Server 2016 for x64-based Systems (Server Core installation) (3206632) (Important)	Windows Server 2016 for x64-based Systems (Server Core installation) (3206632) (Important)	Windows Server 2016 for x64-based Systems (Server Core installation) (3206632) (Important)	Windows Server 2016 for x64-based Systems (Server Core installation) (3206632) (Important)	Not applicable

Microsoft .NET Framework – Security Only Release

Microsoft .NET Framework	
Windows 7 and Windows Server 2008 R2 **Microsoft .NET Framework Updates for 4.6.2 (KB3205406)**	
Bulletin Identifier	**MS16-155**
Aggregate Severity Rating	**Important**
Windows 7 for 32-bit Systems Service Pack 1	Microsoft .NET Framework 4.6.2 (3204805) (Important)
Windows 7 for x64-based Systems Service Pack 1	Microsoft .NET Framework 4.6.2 (3204805) (Important)
Windows Server 2008 R2	
Bulletin Identifier	**MS16-155**
Aggregate Severity Rating	**Important**
Windows Server 2008 R2 for x64-based Systems Service Pack 1	Microsoft .NET Framework 4.6.2 (3204805) (Important)
Windows Server 2008 R2 for Itanium-based Systems Service Pack 1	Microsoft .NET Framework 4.6.2 (3204805) (Important)
Windows 8.1	
Bulletin Identifier	**MS16-155**
Aggregate Severity Rating	**Important**
Windows 8.1 for 32-bit Systems	Microsoft .NET Framework 4.6.2 (3204802) (Important)
Windows 8.1 for x64-based Systems	Microsoft .NET Framework 4.6.2 (3204802) (Important)
Windows Server 2012 and Windows Server 2012 R2	
Bulletin Identifier	**MS16-155**
Aggregate Severity Rating	**Important**
Windows Server 2012	Microsoft .NET Framework 4.6.2 (3204801) (Important)
Windows Server 2012 R2	Microsoft .NET Framework 4.6.2 (3204802) (Important)
Windows RT 8.1	

Bulletin Identifier	**MS16-155**
Aggregate Severity Rating	**Important**
Windows RT 8.1	Microsoft .NET Framework 4.6.2 (3204802) (Important)
Windows 10	
Bulletin Identifier	**MS16-155**
Aggregate Severity Rating	**Important**
Windows 10 Version 1607 for 32-bit Systems (3206632)	Microsoft .NET Framework 4.6.2 (Important)
Windows 10 Version 1607 for x64-based Systems (3206632)	Microsoft .NET Framework 4.6.2 (Important)
Windows Server 2016	
Bulletin Identifier	**MS16-155**
Aggregate Severity Rating	**Important**
Windows Server 2016 for x64-based Systems (3206632)	Microsoft .NET Framework 4.6.2 (Important)
Server Core installation option	
Bulletin Identifier	**MS16-155**
Aggregate Severity Rating	**Important**
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	Microsoft .NET Framework 4.6.2 (3204805) (Important)
Windows Server 2012 (Server Core installation)	Microsoft .NET Framework 4.6.2 (3204801) (Important)
Windows Server 2012 R2 (Server Core installation)	Microsoft .NET Framework 4.6.2 (3204802) (Important)
Windows Server 2016 for x64-based Systems (Server Core installation) (3206632)	Microsoft .NET Framework 4.6.2 (Important)

Note for MS16-155

This bulletin spans more than one software category. See other tables in this section for additional affected software.

Microsoft .NET Framework – Monthly Rollup Release

Microsoft .NET Framework
Windows Vista and Windows Server 2008 **Microsoft .NET Framework Updates for 2.0, 4.5.2, 4.6 (KB3210142)**

Windows Vista	
Bulletin Identifier	**MS16-155**
Aggregate Severity Rating	**Important**
Windows Vista for 32-bit Systems Service Pack 2	Microsoft .NET Framework 3.5 (3210129) (Important) Microsoft .NET Framework 4.5.2 (3210139) (Important) Microsoft .NET Framework 4.6 (3210136) (Important)
Windows Vista for x64-based Systems Service Pack 2	Microsoft .NET Framework 3.5 (3210129) (Important) Microsoft .NET Framework 4.5.2 (3210139) (Important) Microsoft .NET Framework 4.6 (3210136) (Important)
Windows Server 2008	
Bulletin Identifier	**MS16-155**
Aggregate Severity Rating	**Important**
Windows Server 2008 for 32-bit Systems Service Pack 2	Microsoft .NET Framework 3.5 (3210129) (Important) Microsoft .NET Framework 4.5.2 (3210139) (Important) Microsoft .NET Framework 4.6 (3210136) (Important)
Windows Server 2008 for x64-based Systems Service Pack 2	Microsoft .NET Framework 3.5 (3210129) (Important) Microsoft .NET Framework 4.5.2 (3210139) (Important) Microsoft .NET Framework 4.6 (3210136) (Important)
Windows 7 and Windows Server 2008 R2 **Microsoft .NET Framework Updates for 3.5.1, 4.5.2, 4.6/4.6.1, 4.6.2 (KB3205402)**	
Windows 7	

Bulletin Identifier	**MS16-155**
Aggregate Severity Rating	**Important**
Windows 7 for 32-bit Systems Service Pack 1	Microsoft .NET Framework 3.5 (3210131) (Important) Microsoft .NET Framework 4.5.2 (3210139) (Important) Microsoft .NET Framework 4.6/4.6.1 (3210136) (Important) Microsoft .NET Framework 4.6.2 (3205379) (Important)
Windows 7 for x64-based Systems Service Pack 1	Microsoft .NET Framework 3.5 (3210131) (Important) Microsoft .NET Framework 4.5.2 (3210139) (Important) Microsoft .NET Framework 4.6/4.6.1 (3210136) (Important) Microsoft .NET Framework 4.6.2 (3205379) (Important)
Windows Server 2008 R2	
Bulletin Identifier	**MS16-155**
Aggregate Severity Rating	**Important**
Windows Server 2008 R2 for x64-based Systems Service Pack 1	Microsoft .NET Framework 3.5 (3210131) (Important) Microsoft .NET Framework 4.5.2 (3210139) (Important) Microsoft .NET Framework 4.6/4.6.1 (3210136) (Important) Microsoft .NET Framework 4.6.2 (3205379) (Important)
Windows Server 2008 R2 for Itanium-based Systems Service Pack 1	Microsoft .NET Framework 3.5 (3210131) (Important)
Windows Server 2012 **Microsoft .NET Framework Updates for 3.5, 4.5.2, 4.6/4.6.1, 4.6.2 (KB3205403)**	

Bulletin Identifier	**MS16-155**
Aggregate Severity Rating	**Important**
Windows Server 2012	Microsoft .NET Framework 3.5 (3210130) (Important) Microsoft .NET Framework 4.5.2 (3210138) (Important) Microsoft .NET Framework 4.6/4.6.1 (3210133) (Important) Microsoft .NET Framework 4.6.2 (3205377) (Important)
Windows 8.1 and Windows Server 2012 R2 **Microsoft .NET Framework Updates for 3.5, 4.5.2, 4.6/4.6.1, 4.6.2 (KB3205404)**	
Windows 8.1	
Bulletin Identifier	**MS16-155**
Aggregate Severity Rating	**Important**
Windows 8.1 for 32-bit Systems	Microsoft .NET Framework 3.5 (3210132) (Important) Microsoft .NET Framework 4.5.2 (3210137) (Important) Microsoft .NET Framework 4.6/4.6.1 (3210135) (Important) Microsoft .NET Framework 4.6.2 (3205378) (Important)
Windows 8.1 for x64-based Systems	Microsoft .NET Framework 3.5 (3210132) (Important) Microsoft .NET Framework 4.5.2 (3210137) (Important) Microsoft .NET Framework 4.6/4.6.1 (3210135) (Important) Microsoft .NET Framework 4.6.2 (3205378) (Important)
Windows Server 2012 R2	
Windows Server 2012 R2	Microsoft .NET Framework 3.5 (3210132)

	(Important) Microsoft .NET Framework 4.5.2 (3210137) (Important) Microsoft .NET Framework 4.6/4.6.1 (3210135) (Important) Microsoft .NET Framework 4.6.2 (3205378) (Important)
Windows 10	
Bulletin Identifier	**MS16-155**
Aggregate Severity Rating	**Important**
Windows 10 Version 1607 for 32-bit Systems (3206632)	Microsoft .NET Framework 4.6.2 (Important)
Windows 10 Version 1607 for x64-based Systems (3206632)	Microsoft .NET Framework 4.6.2 (Important)
Windows Server 2016	
Bulletin Identifier	**MS16-155**
Aggregate Severity Rating	**Important**
Windows Server 2016 for x64-based Systems (3206632)	Microsoft .NET Framework 4.6.2 (Important)
Server Core installation option	
Bulletin Identifier	**MS16-155**
Aggregate Severity Rating	**Important**
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	Microsoft .NET Framework 3.5 (3210131) (Important) Microsoft .NET Framework 4.6/4.6.1 (3210136) (Important) Microsoft .NET Framework 4.6.2 (3205379) (Important)
Windows Server 2012 (Server Core installation)	Microsoft .NET Framework 3.5 (3210130) (Important) Microsoft .NET Framework 4.5.2 (3210138) (Important) Microsoft .NET Framework 4.6/4.6.1 (3210133) (Important)

	Microsoft .NET Framework 4.6.2 (3205377) (Important)
Windows Server 2012 R2 (Server Core installation)	Microsoft .NET Framework 3.5 (3210132) (Important) Microsoft .NET Framework 4.5.2 (3210137) (Important) Microsoft .NET Framework 4.6/4.6.1 (3210135) (Important) Microsoft .NET Framework 4.6.2 (3205378) (Important)
Windows Server 2016 for x64-based Systems (Server Core installation) (3206632)	Microsoft .NET Framework 4.6.2 (Important)

Note for MS16-155

This bulletin spans more than one software category. See other tables in this section for additional affected software.

Microsoft Office Suites and Software

Microsoft Office 2007	
Bulletin Identifier	**MS16-148**
Aggregate Severity Rating	**Critical**
Microsoft Office 2007 Service Pack 3	Microsoft Excel 2007 Service Pack 3 (3128019) (Important) Microsoft Word 2007 Service Pack 3 (3128025) (Important) Microsoft Office 2007 Service Pack 3 (2883033) (Critical) Microsoft Office 2007 Service Pack 3 (3128020) (Important)
Microsoft Office 2010	
Bulletin Identifier	**MS16-148**
Aggregate Severity Rating	**Critical**
Microsoft Office 2010 Service Pack 2 (32-bit editions)	Microsoft Office 2010 Service Pack 2 (32-bit editions) (3128032) (Important) Microsoft Office 2010 Service Pack 2 (32-bit editions)

	(3118380) (Important) Microsoft Office 2010 Service Pack 2 (32-bit editions) (2889841) (Critical) Microsoft Excel 2010 Service Pack 2 (32-bit editions) (3128037) (Important) Microsoft Publisher 2010 Service Pack 2 (32-bit editions) (3114395) (Important) Microsoft Word 2010 Service Pack 2 (32-bit editions) (3128034) (Important)
Microsoft Office 2010 Service Pack 2 (64-bit editions)	Microsoft Office 2010 Service Pack 2 (64-bit editions) (3128032) (Important) Microsoft Office 2010 Service Pack 2 (64-bit editions) (3118380) (Important) Microsoft Office 2010 Service Pack 2 (64-bit editions) (2889841) (Critical) Microsoft Excel 2010 Service Pack 2 (64-bit editions) (3128037) (Important) Microsoft Publisher 2010 Service Pack 2 (64-bit editions) (3114395) (Important) Microsoft Word 2010 Service Pack 2 (64-bit editions) (3128034) (Important)
Microsoft Office 2013	
Bulletin Identifier	**MS16-148**
Aggregate Severity Rating	**Important**
Microsoft Office 2013 Service Pack 1 (32-bit editions)	Microsoft Excel 2013 Service Pack 1 (32-bit editions) (3128008) (Important) Microsoft Office 2013 Service Pack 1 (32-bit editions) (3127968) (Important)
Microsoft Office 2013 Service Pack 1 (64-bit editions)	Microsoft Excel 2013 Service Pack 1 (64-bit editions) (3128008) (Important) Microsoft Office 2013 Service Pack 1 (64-bit editions) (3127968) (Important)
Microsoft Office 2013 RT	

Bulletin Identifier	**MS16-148**
Aggregate Severity Rating	**Important**
Microsoft Office 2013 RT Service Pack 1	Microsoft Excel 2013 RT Service Pack 1 (3128008) (Important) Microsoft Office 2013 RT Service Pack 1 (3127968) (Important)
Microsoft Office 2016	
Bulletin Identifier	**MS16-148**
Aggregate Severity Rating	**Important**
Microsoft Office 2016 (32-bit edition)	Microsoft Excel 2016 (32-bit edition) (3128016) (Important) Microsoft Office 2016 (32-bit edition) (3127986) (Important) Microsoft Office 2016 (32-bit edition) (Important)[1]
Microsoft Office 2016 (64-bit edition)	Microsoft Excel 2016 (64-bit edition) (3128016) (Important) Microsoft Office 2016 (64-bit edition) (3127986) (Important) Microsoft Office 2016 (64-bit edition) (Important)[1]
Microsoft Office for Mac 2011	
Bulletin Identifier	**MS16-148**
Aggregate Severity Rating	**Important**
	Microsoft Office for Mac 2011 (3198808) (Important) Microsoft Excel for Mac 2011 (3198808) (Important) Microsoft Word for Mac 2011 (3198808) (Important)
Microsoft Office 2016 for Mac	
Bulletin Identifier	**MS16-148**
Aggregate Severity Rating	**Important**

	Microsoft Office 2016 for Mac (3198800) (Important) Microsoft Excel 2016 for Mac (3198800) (Important)
Other Office for Mac Software	
Bulletin Identifier	**MS16-148**
Aggregate Severity Rating	**Important**
Microsoft Auto Updater for Mac	Microsoft Auto Updater for Mac[2] (Important)
Other Office Software	
Bulletin Identifier	**MS16-148**
Aggregate Severity Rating	**Critical**
Microsoft Office Compatibility Pack Service Pack 3	Microsoft Office Compatibility Pack Service Pack 3 (3128022) (Important) Microsoft Office Compatibility Pack Service Pack 3 (3128024) (Important)
Microsoft Excel Viewer	Microsoft Excel Viewer (3128023) (Important)
Microsoft Word Viewer	Microsoft Word Viewer (3128044) (Important) Microsoft Word Viewer (3127995) (Critical)

[1]This entry references the Click-to-Run (C2R) version only.

Note for MS16-148

This bulletin spans more than one software category. See other tables in this section for additional affected software.

Microsoft Office Services and Web Apps

Microsoft SharePoint Server 2007	
Bulletin Identifier	**MS16-148**
Aggregate Severity Rating	**Important**
Microsoft SharePoint Server 2007 Service Pack 3 (32-bit edition)	Excel Services

	(3127892) (Important)
Microsoft SharePoint Server 2007 Service Pack 3 (64-bit edition)	Excel Services (3127892) (Important)
Microsoft SharePoint Server 2010	
Bulletin Identifier	**MS16-148**
Aggregate Severity Rating	**Important**
Microsoft SharePoint Server 2010 Service Pack 2	Excel Services (3128029) (Important)
Microsoft SharePoint Server 2010 Service Pack 2	Word Automation Services (3128026) (Important)
Microsoft Office Web Apps 2010	
Bulletin Identifier	**MS16-148**
Aggregate Severity Rating	**Important**
Microsoft Office Web Apps 2010 Service Pack 2	Microsoft Office Web Apps 2010 Service Pack 2 (3128035) (Important)

Note for MS16-148

This bulletin spans more than one software category. See other tables in this section for additional affected software.

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 (December13, 2016): Bulletin Summary published.
- V1.1 (December21, 2016): For MS16-148, CVE-2016-7298 has been changed to CVE-2016-7274. This is an informational change only. Customers who have successfully installed the updates do not need to take any further action.
- V1.2 (December21, 2016): The December 13, 2016, Security and Quality Rollups updates 3210137 and 3210138 contain a known issue that affects the .NET Framework 4.5.2 running on Windows 8.1, Windows Server 2012 R2, and Windows Server 2012. The issue was also present in the November 15, 2016, Preview of Quality rollup updates that were superseded by the December 13, 2016 Rollup updates.

The issue causes applications that connect to an instance of Microsoft SQL Server on the same computer to generate the following error message: “provider: Shared Memory Provider, error: 15 - Function not supported”
For more information please refer to Knowledge Based Article 3214106

Page generated 2016-12-21 14:08-08:00.