Microsoft Security Bulletin Summary for October 2016

Published: October 11, 2016 | Updated: September 12, 2017

Version: 3.0

This bulletin summary lists security bulletins released for October 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
MS16-118	**Cumulative Security Update for Internet Explorer (3192887)** 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	3185614 3185611 3188966 3192392 3192393 3192391	Microsoft Windows, Internet Explorer
MS16-119	**Cumulative Security Update for Microsoft Edge (3192890)** 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	3185614 3185611 3188966	Microsoft Windows, Microsoft Edge

MS16-120	**Security Update for Microsoft Graphics Component (3192884)** This security update resolves vulnerabilities in Microsoft Windows, Microsoft .NET Framework, Microsoft Office, Skype for Business, Silverlight, and Microsoft Lync. The most serious of these 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	3185614 3185611 3188966 3192392 3192393 3192391	Microsoft Windows, Microsoft .NET Framework, Microsoft Office, Skype for Business, and Microsoft Lync.
MS16-121	**Security Update for Microsoft Office (3194063)** This security update resolves a vulnerability in Microsoft Office. An Office RTF remote code execution vulnerability exists in Microsoft Office software when the Office software fails to properly handle RTF files. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user.	Critical Remote Code Execution	May require restart	---------	Microsoft Office, Microsoft Office Services and Web Apps
MS16-122	**Security Update for Microsoft Video Control (3195360)** This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if 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 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.	Critical Remote Code Execution	Requires restart	3185614 3185611 3188966 3192392 3192393 3192391	Microsoft Windows
MS16-123	**Security Update for Windows Kernel-Mode Drivers (3192892)** This security update resolves vulnerabilities in Microsoft Windows. The more 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	3185614 3185611 3188966 3192392 3192393 3192391	Microsoft Windows
MS16-124	**Security Update for Windows Registry (3193227)** This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities could allow elevation of privilege if an attacker can access sensitive registry information.	Important Elevation of Privilege	Requires restart	3185614 3185611 3188966 3192392 3192393 3192391	Microsoft Windows
MS16-125	**Security Update for Diagnostics Hub (3193229)** This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if an attacker logs on to an affected system and runs a specially crafted application.	Important Elevation of Privilege	Requires restart	3185614 3185611 3188966	Microsoft Windows

MS16-126	**Security Update for Microsoft Internet Messaging API (3196067)** This security update resolves a vulnerability in Microsoft Windows. An information disclosure vulnerability exists when the Microsoft Internet Messaging API improperly handles objects in memory. An attacker who successfully exploited this vulnerability could test for the presence of files on disk.	Moderate Information Disclosure	Requires restart	3185614 3185611 3188966 3192392 3192393 3192391	Microsoft Windows
MS16-127	**Security Update for Adobe Flash Player (3194343)** 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, and Windows 10.	Critical Remote Code Execution	Requires restart	---------	Microsoft Windows, Adobe Flash Player
MS16-128	**Security Update for Adobe Flash Player (3201860**) 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, and Windows 10.	Critical Remote Code Execution	Requires restart	---------	Microsoft Windows, Adobe Flash Player

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
MS16-118: Cumulative Security Update for Internet Explorer (3192887)				
CVE-2016-3267	Microsoft Browser Information Disclosure Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-3298	Microsoft Browser Information Disclosure Vulnerability	0 - Exploitation Detected	0 - Exploitation Detected	Not applicable
CVE-2016-3331	Microsoft Browser Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable

CVE-2016-3382	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-3383	Internet Explorer Memory Corruption Vulnerability	4 - Not affected	1 - Exploitation More Likely	Not applicable
CVE-2016-3384	Internet Explorer Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-3385	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-3387	Microsoft Browser Elevation of Privilege Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-3388	Microsoft Browser Elevation of Privilege Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-3390	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-3391	Microsoft Browser Information Disclosure Vulnerability	3 - Exploitation Unlikely	3 - Exploitation Unlikely	Not applicable
MS16-119: Cumulative Security Update for Microsoft Edge (3192890)				
CVE-2016-3267	Microsoft Browser Information Disclosure Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-3331	Microsoft Browser Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-3382	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-3386	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-3387	Microsoft Browser Elevation of	1 - Exploitation More Likely	4 - Not affected	Not applicable

	Privilege Vulnerability			
CVE-2016-3388	Microsoft Browser Elevation of Privilege Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-3389	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-3390	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-3391	Microsoft Browser Information Disclosure Vulnerability	3 - Exploitation Unlikely	4 - Not affected	Not applicable
CVE-2016-3392	Microsoft Edge Security Feature Bypass	3 - Exploitation Unlikely	4 - Not affected	Not applicable
CVE-2016-7189	Scripting Engine Remote Code Execution Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-7190	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-7194	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
MS16-120: Security Update for Microsoft Graphics Component (3192884)				
CVE-2016-3209	True Type Font Parsing Information Disclosure Vulnerability	2 - Exploitation Less Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-3262	GDI+ Information Disclosure Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2016-3263	GDI+ Information Disclosure Vulnerability	4 - Not affected	2 - Exploitation Less Likely	Temporary
CVE-2016-3270	Win32k Elevation of Privilege Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-3393	Windows Graphics Component RCE Vulnerability	1 - Exploitation More Likely	0 - Exploitation Detected	Permanent

CVE-2016-3396	GDI+ Remote Code Execution Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-7182	True Type Font Parsing Elevation of Privilege Vulnerability	2 - Exploitation Less Likely	1 - Exploitation More Likely	Not applicable
MS16-121: Security Update for Microsoft Office (3194063)				
CVE-2016-7193	Microsoft Office Memory Corruption Vulnerability	0 - Exploitation Detected	0 - Exploitation Detected	Not applicable
MS16-122: Security Update for Microsoft Video Control (3195360)				
CVE-2016-0142	Microsoft Video Control Remote Code Execution Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
MS16-123: Security Update for Windows Kernel-Mode Drivers (3192892)				
CVE-2016-3266	Win32k Elevation of Privilege Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-3341	Windows Transaction Manager Elevation of Privilege Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2016-3376	Win32k Elevation of Privilege Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2016-7185	Win32k Elevation of Privilege Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Permanent
CVE-2016-7211	Win32k Elevation of Privilege Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
MS16-124: Security Update for Windows Registry (3193227)				
CVE-2016-0070	Windows Kernel Local Elevation of Privilege	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2016-0073	Windows Kernel Local Elevation of Privilege	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2016-0075	Windows Kernel Local Elevation of Privilege	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2016-0079	Windows Kernel Local Elevation of	2 - Exploitation Less Likely	4 - Not affected	Not applicable

	Privilege			
MS16-125: Security Update for Diagnostics Hub (3193229)				
CVE-2016-7188	Windows Diagnostics Hub Elevation of Privilege	1 - Exploitation More Likely	4 - Not affected	Not applicable
MS16-126: Security Update for Microsoft Internet Messaging API (3196067)				
CVE-2016-3298	Internet Explorer Information Disclosure Vulnerability	4 - Not affected	0 - Exploitation Detected	Not applicable
MS16-127: Security Update for Adobe Flash Player (3194343)				
APSB16-32	See Adobe Security Bulletin APSB16-32 for vulnerability severity and update priority ratings.	----------	----------	Not applicable
MS16-128: Security Update for Adobe Flash Player (3201860)				
APSB16-36	See Adobe Security Bulletin APSB16-36 for vulnerability severity and update priority ratings.	----------	----------	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	**MS16-118**	**MS16-119**	**MS16-120**	**MS16-122**	**MS16-123**
Aggregate Severity Rating	**Critical**	**None**	**Critical**	**Critical**	**Important**
Windows Vista Service Pack 2	Internet Explorer 9 (3191492) (Critical)	Not applicable	Windows Vista Service Pack 2 (3191203) (Critical)	Windows Vista Service Pack 2 (3190847) (Critical)	Windows Vista Service Pack 2 (3191203) (Important)

					Windows Vista Service Pack 2 (3183431) (Important)
Windows Vista x64 Edition Service Pack 2	Internet Explorer 9 (3191492) (Critical)	Not applicable	Windows Vista x64 Edition Service Pack 2 (3191203) (Critical)	Windows Vista x64 Edition Service Pack 2 (3190847) (Critical)	Windows Vista x64 Edition Service Pack 2 (3191203) (Important) Windows Vista x64 Edition Service Pack 2 (3183431) (Important)
Windows Server 2008					
Bulletin Identifier	**MS16-118**	**MS16-119**	**MS16-120**	**MS16-122**	**MS16-123**
Aggregate Severity Rating	**Moderate**	**None**	**Critical**	**None**	**Important**
Windows Server 2008 for 32-bit Systems Service Pack 2	Internet Explorer 9 (3191492) (Moderate)	Not applicable	Windows Server 2008 for 32-bit Systems Service Pack 2 (3191203) (Critical)	Not applicable	Windows Server 2008 for 32-bit Systems Service Pack 2 (3191203) (Important) Windows Server 2008 for 32-bit Systems Service Pack 2 (3183431) (Important)
Windows Server 2008 for x64-based Systems Service Pack 2	Internet Explorer 9 (3191492) (Moderate)	Not applicable	Windows Server 2008 for x64-based Systems Service Pack 2 (3191203) (Critical)	Not applicable	Windows Server 2008 for x64-based Systems Service Pack 2 (3191203) (Important) Windows Server 2008 for x64-based Systems Service Pack 2 (3183431) (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 (3191203) (Critical)	Not applicable	Windows Server 2008 for Itanium-based Systems Service Pack 2 (3191203) (Important) Windows Server 2008 for Itanium-based Systems Service Pack 2 (3183431) (Important)

Windows 7					
Bulletin Identifier	**MS16-118**	**MS16-119**	**MS16-120**	**MS16-122**	**MS16-123**
Aggregate Severity Rating	**Critical**	**None**	**Critical**	**Critical**	**Important**
Windows 7 for 32-bit Systems Service Pack 1 Security Only	Internet Explorer 11 (3192391) (Critical)	Not applicable	Windows 7 for 32-bit Systems Service Pack 1 (3192391) (Critical)	Windows 7 for 32-bit Systems Service Pack 1 (3192391) (Critical)	Windows 7 for 32-bit Systems Service Pack 1 (3192391) (Important)
Windows 7 for 32-bit Systems Service Pack 1 Monthly Roll Up	Internet Explorer 11 (3185330) (Critical)	Not applicable	Windows 7 for 32-bit Systems Service Pack 1 (3185330) (Critical)	Windows 7 for 32-bit Systems Service Pack 1 (3185330) (Critical)	Windows 7 for 32-bit Systems Service Pack 1 (3185330) (Important)
Windows 7 for x64-based Systems Service Pack 1 Security Only	Internet Explorer 11 (3192391) (Critical)	Not applicable	Windows 7 for x64-based Systems Service Pack 1 (3192391) (Critical)	Windows 7 for x64-based Systems Service Pack 1 (3192391) (Critical)	Windows 7 for x64-based Systems Service Pack 1 (3192391) (Important)
Windows 7 for x64-based Systems Service Pack 1 Monthly Roll Up	Internet Explorer 11 (3185330) (Critical)	Not applicable	Windows 7 for x64-based Systems Service Pack 1 (3185330) (Critical)	Windows 7 for x64-based Systems Service Pack 1 (3185330) (Critical)	Windows 7 for x64-based Systems Service Pack 1 (3185330) (Important)
Windows Server 2008 R2					
Bulletin Identifier	**MS16-118**	**MS16-119**	**MS16-120**	**MS16-122**	**MS16-123**
Aggregate Severity Rating	**Moderate**	**None**	**Critical**	**None**	**Important**
Windows Server 2008 R2 for x64-based Systems Service Pack 1 Security Only	Internet Explorer 11 (3192391) (Moderate)	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3192391) (Critical)	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3192391) (Important)
Windows Server 2008 R2 for x64-based Systems Service Pack 1 Monthly Roll Up	Internet Explorer 11 (3185330) (Moderate)	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3185330) (Critical)	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3185330) (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 (3192391) (Critical)	Not applicable	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3192391) (Important)
Windows Server 2008 R2 for Itanium-	Not applicable	Not applicable	Windows Server 2008	Not applicable	Windows Server

based Systems Service Pack 1 Monthly Rollup			R2 for Itanium-based Systems Service Pack 1 (3185330) (Critical)		2008 R2 for Itanium-based Systems Service Pack 1 (3185330) (Important)
Windows 8.1					
Bulletin Identifier	**MS16-118**	**MS16-119**	**MS16-120**	**MS16-122**	**MS16-123**
Aggregate Severity Rating	**Critical**	**None**	**Critical**	**Critical**	**Important**
Windows 8.1 for 32-bit Systems Security Only	Internet Explorer 11 (3192392) (Critical)	Not applicable	Windows 8.1 for 32-bit Systems (3192392) (Critical)	Windows 8.1 for 32-bit Systems (3192392) (Critical)	Windows 8.1 for 32-bit Systems (3192392) (Important)
Windows 8.1 for 32-bit Systems Monthly Roll Up	Internet Explorer 11 (3185331) (Critical)	Not applicable	Windows 8.1 for 32-bit Systems (3185331) (Critical)	Windows 8.1 for 32-bit Systems (3185331) (Critical)	Windows 8.1 for 32-bit Systems (3185331) (Important)
Windows 8.1 for x64-based Systems Security Only	Internet Explorer 11 (3192392) (Critical)	Not applicable	Windows 8.1 for x64-based Systems (3192392) (Critical)	Windows 8.1 for x64-based Systems (3192392) (Critical)	Windows 8.1 for x64-based Systems (3192392) (Important)
Windows 8.1 for x64-based Systems Monthly Roll Up	Internet Explorer 11 (3185331) (Critical)	Not applicable	Windows 8.1 for x64-based Systems (3185331) (Critical)	Windows 8.1 for x64-based Systems (3185331) (Critical)	Windows 8.1 for x64-based Systems (3185331) (Important)
Windows Server 2012 and Windows Server 2012 R2					
Bulletin Identifier	**MS16-118**	**MS16-119**	**MS16-120**	**MS16-122**	**MS16-123**
Aggregate Severity Rating	**Moderate**	**None**	**Critical**	**None**	**Important**
Windows Server 2012 Security Only	Internet Explorer 10 (3192393) (Moderate)	Not applicable	Windows Server 2012 (3192393) (Critical)	Not applicable	Windows Server 2012 (3192393) (Important)
Windows Server 2012 Monthly Roll Up	Internet Explorer 10 (3185332) (Moderate)	Not applicable	Windows Server 2012 (3185332) (Critical)	Not applicable	Windows Server 2012 (3185332) (Important)
Windows Server 2012 R2 Security Only	Internet Explorer 11 (3192392) (Moderate)	Not applicable	Windows Server 2012 R2 (3192392) (Critical)	Not applicable	Windows Server 2012 R2 (3192392) (Important)
Windows Server 2012 R2 Monthly Roll Up	Internet Explorer 11 (3185331) (Moderate)	Not applicable	Windows Server 2012 R2 (3185331) (Critical)	Not applicable	Windows Server 2012 R2 (3185331) (Important)

Windows RT 8.1					
Bulletin Identifier	**MS16-118**	**MS16-119**	**MS16-120**	**MS16-122**	**MS16-123**
Aggregate Severity Rating	**Critical**	**None**	**Critical**	**Critical**	**Important**
Windows RT 8.1 Monthly Roll Up	Internet Explorer 11 (3185331) (Critical)	Not applicable	Windows RT 8.1 (3185331) (Critical)	Windows RT 8.1 (3185331) (Critical)	Windows RT 8.1 (3185331) (Important)
Windows 10					
Bulletin Identifier	**MS16-118**	**MS16-119**	**MS16-120**	**MS16-122**	**MS16-123**
Aggregate Severity Rating	**Critical**	**Critical**	**Critical**	**Critical**	**Important**
Windows 10 for 32-bit Systems	Internet Explorer 11 (3192440) (Critical)	Microsoft Edge (3192440) (Critical)	Windows 10 for 32-bit Systems (3192440) (Critical)	Windows 10 for 32-bit Systems (3192440) (Critical)	Windows 10 for 32-bit Systems (3192440) (Important)
Windows 10 for x64-based Systems	Internet Explorer 11 (3192440) (Critical)	Microsoft Edge (3192440) (Critical)	Windows 10 for x64-based Systems (3192440) (Critical)	Windows 10 for x64-based Systems (3192440) (Critical)	Windows 10 for x64-based Systems (3192440) (Important)
Windows 10 Version 1511 for 32-bit Systems	Internet Explorer 11 (3192441) (Critical)	Microsoft Edge (3192441) (Critical)	Windows 10 Version 1511 for 32-bit Systems (3192441) (Critical)	Windows 10 Version 1511 for 32-bit Systems (3192441) (Critical)	Windows 10 Version 1511 for 32-bit Systems (3192441) (Important)
Windows 10 Version 1511 for x64-based Systems	Internet Explorer 11 (3192441) (Critical)	Microsoft Edge (3192441) (Critical)	Windows 10 Version 1511 for x64-based Systems (3192441) (Critical)	Windows 10 Version 1511 for x64-based Systems (3192441) (Critical)	Windows 10 Version 1511 for x64-based Systems (3192441) (Important)
Windows 10 Version 1607 for 32-bit Systems	Internet Explorer 11 (3194798) (Critical)	Microsoft Edge (3194798) (Critical)	Windows 10 Version 1607 for x64-based Systems (3194798) (Critical)	Windows 10 Version 1607 for x64-based Systems (3194798) (Critical)	Windows 10 Version 1607 for x64-based Systems (3194798) (Important)
Windows 10 Version 1607 for x64-based Systems	Internet Explorer 11 (3194798) (Critical)	Microsoft Edge (3194798) (Critical)	Windows 10 Version 1607 for x64-based Systems (3194798) (Critical)	Windows 10 Version 1607 for x64-based Systems (3194798) (Critical)	Windows 10 Version 1607 for x64-based Systems (3194798) (Important)
Windows 10 Version 1703 for 32-bit Systems	Not applicable	Not applicable	Not applicable	Not applicable	Windows 10 Version 1607 for x64-based Systems (4038788) (Important)

Windows 10 Version 1703 for x64-based Systems	Not applicable	Not applicable	Not applicable	Not applicable	Windows 10 Version 1607 for x64-based Systems (4038788) (Important)
Server Core installation option					
Bulletin Identifier	**MS16-118**	**MS16-119**	**MS16-120**	**MS16-122**	**MS16-123**
Aggregate Severity Rating	**None**	**None**	**Critical**	**None**	**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) (3191203) (Critical)	Not applicable	Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (3191203) (Important) Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (3183431) (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) (3191203) (Critical)	Not applicable	Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) (3191203) (Important) Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) (3183431) (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) (3192391) (Critical)	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3192391) (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) (3185330) (Critical)	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3185330) (Important)

Windows Server 2012 (Server Core installation) Security Only	Not applicable	Not applicable	Windows Server 2012 (Server Core installation) (3192393) (Critical)	Not applicable	Windows Server 2012 (Server Core installation) (3192393) (Important)
Windows Server 2012 (Server Core installation) Monthly Rollup	Not applicable	Not applicable	Windows Server 2012 (Server Core installation) (3185332) (Critical)	Not applicable	Windows Server 2012 (Server Core installation) (3185332) (Important)
Windows Server 2012 R2 (Server Core installation) Security Only	Not applicable	Not applicable	Windows Server 2012 R2 (Server Core installation) (3192392) (Critical)	Not applicable	Windows Server 2012 R2 (Server Core installation) (3192392) (Important)
Windows Server 2012 R2 (Server Core installation) Monthly Rollup	Not applicable	Not applicable	Windows Server 2012 R2 (Server Core installation) (3185331) (Critical)	Not applicable	Windows Server 2012 R2 (Server Core installation) (3185331) (Important)

Windows Operating Systems and Components (Table 2 of 2)

Windows Vista					
Bulletin Identifier	**MS16-124**	**MS16-125**	**MS16-126**	**MS16-127**	**MS16-128**
Aggregate Severity Rating	**Important**	**None**	**Moderate**	**None**	**None**
Windows Vista Service Pack 2	Windows Vista Service Pack 2 (3191256) (Important)	Not applicable	Windows Vista Service Pack 2 (3193515) (Moderate)	Not applicable	Not applicable
Windows Vista x64 Edition Service Pack 2	Windows Vista x64 Edition Service Pack 2 (3191256) (Important)	Not applicable	Windows Vista x64 Edition Service Pack 2 (3193515) (Moderate)	Not applicable	Not applicable
Windows Server 2008					
Bulletin Identifier	**MS16-124**	**MS16-125**	**MS16-126**	**MS16-127**	**MS16-128**
Aggregate Severity Rating	**Important**	**None**	**Low**	**None**	**None**
Windows Server 2008 for 32-bit Systems Service Pack 2	Windows Server 2008 for 32-bit Systems Service Pack 2 (3191256) (Important)	Not applicable	Windows Server 2008 for 32-bit Systems Service Pack 2 (3193515) (Low)	Not applicable	Not applicable
Windows Server 2008 for x64-based Systems Service Pack 2	Windows Server 2008 for x64-based Systems Service Pack 2	Not applicable	Windows Server 2008 for x64-based Systems Service Pack 2	Not applicable	Not applicable

	(3191256) (Important)		(3193515) (Low)		
Windows Server 2008 for Itanium-based Systems Service Pack 2	Windows Server 2008 for Itanium-based Systems Service Pack 2 (3191256) (Important)	Not applicable	Windows Server 2008 for Itanium-based Systems Service Pack 2 (3193515) (Low)	Not applicable	Not applicable
Windows 7					
Bulletin Identifier	**MS16-124**	**MS16-125**	**MS16-126**	**MS16-127**	**MS16-128**
Aggregate Severity Rating	**Important**	**None**	**Moderate**	**None**	**None**
Windows 7 for 32-bit Systems Service Pack 1 Security Only	Windows 7 for 32-bit Systems Service Pack 1 (3192391) (Important)	Not applicable	Windows 7 for 32-bit Systems Service Pack 1 (3192391) (Moderate)	Not applicable	Not applicable
Windows 7 for 32-bit Systems Service Pack 1 Monthly Roll Up	Windows 7 for 32-bit Systems Service Pack 1 (3185330) (Important)	Not applicable	Windows 7 for 32-bit Systems Service Pack 1 (3185330) (Moderate)	Not applicable	Not applicable
Windows 7 for x64-based Systems Service Pack 1 Security Only	Windows 7 for x64-based Systems Service Pack 1 (3192391) (Important)	Not applicable	Windows 7 for x64-based Systems Service Pack 1 (3192391) (Moderate)	Not applicable	Not applicable
Windows 7 for x64-based Systems Service Pack 1 Monthly Roll Up	Windows 7 for x64-based Systems Service Pack 1 (3185330) (Important)	Not applicable	Windows 7 for x64-based Systems Service Pack 1 (3185330) (Moderate)	Not applicable	Not applicable
Windows Server 2008 R2					
Bulletin Identifier	**MS16-124**	**MS16-125**	**MS16-126**	**MS16-127**	**MS16-128**
Aggregate Severity Rating	**Important**	**None**	**Low**	**None**	**None**
Windows Server 2008 R2 for x64-based Systems Service Pack 1 Security Only	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3192391) (Important)	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3192391) (Low)	Not applicable	Not applicable
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 (3185330) (Important)	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3185330) (Low)	Not applicable	Not applicable
Windows Server 2008 R2 for Itanium-	Windows Server	Not applicable	Windows Server	Not applicable	Not applicable

based Systems Service Pack 1 Security Only	2008 R2 for Itanium-based Systems Service Pack 1 (3192391) (Important)		2008 R2 for Itanium-based Systems Service Pack 1 (3192391) (Low)		
Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 Monthly Rollup	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3185330) (Important)	Not applicable	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3185330) (Low)	Not applicable	Not applicable
Windows 8.1					
Bulletin Identifier	**MS16-124**	**MS16-125**	**MS16-126**	**MS16-127**	**MS16-128**
Aggregate Severity Rating	**Important**	**None**	**None**	**Critical**	**Critical**
Windows 8.1 for 32-bit Systems Security Only	Windows 8.1 for 32-bit Systems (3192392) (Important)	Not applicable	Not applicable	Adobe Flash Player (3194343) (Critical)	Adobe Flash Player (3201860) (Critical)
Windows 8.1 for 32-bit Systems Monthly Roll Up	Windows 8.1 for 32-bit Systems (3185331) (Important)	Not applicable	Not applicable	Not applicable	Not applicable
Windows 8.1 for x64-based Systems Security Only	Windows 8.1 for x64-based Systems (3192392) (Important)	Not applicable	Not applicable	Adobe Flash Player (3194343) (Critical)	Adobe Flash Player (3201860) (Critical)
Windows 8.1 for x64-based Systems Monthly Roll Up	Windows 8.1 for x64-based Systems (3185331) (Important)	Not applicable	Not applicable	Not applicable	Not applicable
Windows Server 2012 and Windows Server 2012 R2					
Bulletin Identifier	**MS16-124**	**MS16-125**	**MS16-126**	**MS16-127**	**MS16-128**
Aggregate Severity Rating	**Important**	**None**	**None**	**Moderate**	**Moderate**
Windows Server 2012 Security Only	Windows Server 2012 (3192393) (Important)	Not applicable	Not applicable	Adobe Flash Player (3194343) (Moderate)	Adobe Flash Player (3201860) (Moderate)
Windows Server 2012 Monthly Roll Up	Windows Server 2012 (3185332) (Important)	Not applicable	Not applicable	Not applicable	Not applicable
Windows Server 2012 R2 Security Only	Windows Server 2012 R2 (3192392) (Important)	Not applicable	Not applicable	Adobe Flash Player (3194343) (Moderate)	Adobe Flash Player (3201860) (Moderate)
Windows Server 2012 R2	Windows Server	Not applicable	Not applicable	Not applicable	Not applicable

Monthly Roll Up	2012 R2 (3185331) (Important)				
Windows RT 8.1					
Bulletin Identifier	**MS16-124**	**MS16-125**	**MS16-126**	**MS16-127**	**MS16-128**
Aggregate Severity Rating	**Important**	**None**	**None**	**Critical**	**Critical**
Windows RT 8.1 Monthly Roll Up	Windows RT 8.1 (3185331) (Important)	Not applicable	Not applicable	Adobe Flash Player (3194343) (Critical)	Adobe Flash Player (3201860) (Critical)
Windows 10					
Bulletin Identifier	**MS16-124**	**MS16-125**	**MS16-126**	**MS16-127**	**MS16-128**
Aggregate Severity Rating	**Important**	**Important**	**None**	**Critical**	**Critical**
Windows 10 for 32-bit Systems	Windows 10 for 32-bit Systems (3192440) (Important)	Windows 10 for 32-bit Systems (3192440) (Important)	Not applicable	Adobe Flash Player (3194343) (Critical)	Adobe Flash Player (3201860) (Critical)
Windows 10 for x64-based Systems	Windows 10 for x64-based Systems (3192440) (Important)	Windows 10 for x64-based Systems (3192440) (Important)	Not applicable	Adobe Flash Player (3194343) (Critical)	Adobe Flash Player (3201860) (Critical)
Windows 10 Version 1511 for 32-bit Systems	Windows 10 Version 1511 for 32-bit Systems (3192441) (Important)	Windows 10 Version 1511 for 32-bit Systems (3192441) (Important)	Not applicable	Adobe Flash Player (3194343) (Critical)	Adobe Flash Player (3201860) (Critical)
Windows 10 Version 1511 for x64-based Systems	Windows 10 Version 1511 for x64-based Systems (3192441) (Important)	Windows 10 Version 1511 for x64-based Systems (3192441) (Important)	Not applicable	Adobe Flash Player (3194343) (Critical)	Adobe Flash Player (3201860) (Critical)
Windows 10 Version 1607 for 32-bit Systems	Windows 10 Version 1607 for x64-based Systems (3194798) (Important)	Windows 10 Version 1607 for x64-based Systems (3194798) (Important)	Not applicable	Adobe Flash Player (3194343) (Critical)	Adobe Flash Player (3201860) (Critical)
Windows 10 Version 1607 for x64-based Systems	Windows 10 Version 1607 for x64-based Systems (3194798) (Important)	Windows 10 Version 1607 for x64-based Systems (3194798) (Important)	Not applicable	Adobe Flash Player (3194343) (Critical)	Adobe Flash Player (3201860) (Critical)
Server Core installation option					
Bulletin	**MS16-124**	**MS16-125**	**MS16-126**	**MS16-127**	**MS16-128**

Identifier					
Aggregate Severity Rating	**Important**	**None**	**None**	**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) (3191256) (Important)	Not applicable	Not applicable	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) (3191256) (Important)	Not applicable	Not applicable	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) (3192391) (Important)	Not applicable	Not applicable	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) (3185330) (Important)	Not applicable	Not applicable	Not applicable	Not applicable
Windows Server 2012 (Server Core installation) Security Only	Windows Server 2012 (Server Core installation) (3192393) (Important)	Not applicable	Not applicable	Not applicable	Not applicable
Windows Server 2012 (Server Core installation) Monthly Rollup	Windows Server 2012 (Server Core installation) (3185332) (Important)	Not applicable	Not applicable	Not applicable	Not applicable
Windows Server 2012 R2 (Server Core installation) Security Only	Windows Server 2012 R2 (Server Core installation) (3192392) (Important)	Not applicable	Not applicable	Not applicable	Not applicable
Windows Server 2012 R2 (Server Core installation) Monthly Rollup	Windows Server 2012 R2 (Server Core installation) (3185331) (Important)	Not applicable	Not applicable	Not applicable	Not applicable

Microsoft .NET Framework – Security Only Release

Microsoft .NET Framework	
Windows Vista **Microsoft .NET Framework Updates for 3.0, 4.5.2 and 4.6 for Vista and Server 2008 (KB3188736)**	
Bulletin Identifier	**MS16-120**
Aggregate Severity Rating	**Important**
Windows Vista Service Pack 2	Microsoft .NET Framework 3.0 Service Pack 2 (3188726) (Important)
Windows Vista Service Pack 2	Microsoft .NET Framework 4.5.2 (3189039) (Important)
Windows Vista Service Pack 2	Microsoft .NET Framework 4.6 (3189040) (Important)
Windows Vista x64 Edition Service Pack 2	Microsoft .NET Framework 3.0 Service Pack 2 (3188726) (Important)
Windows Vista x64 Edition Service Pack 2	Microsoft .NET Framework 4.5.2 (3189039) (Important)
Windows Vista x64 Edition Service Pack 2	Microsoft .NET Framework 4.6 (3189040) (Important)
Windows Server 2008 **Microsoft .NET Framework Updates for 3.0, 4.5.2 and 4.6 for Vista and Server 2008 (KB3188736)**	
Bulletin Identifier	**MS16-120**
Aggregate Severity Rating	**Important**
Windows Server 2008 for 32-bit Systems Service Pack 2	Microsoft .NET Framework 3.0 Service Pack 2 (3188726) (Important)
Windows Server 2008 for 32-bit Systems Service Pack 2	Microsoft .NET Framework 4.5.2 (3189039) (Important)
Windows Server 2008 for 32-bit Systems Service Pack 2	Microsoft .NET Framework 4.6 (3189040) (Important)
Windows Server 2008 for x64-based Systems Service Pack 2	Microsoft .NET Framework 3.0 Service Pack 2 (3188726) (Important)
Windows Server 2008 for x64-based Systems Service Pack 2	Microsoft .NET Framework 4.5.2 (3189039) (Important)
Windows Server 2008 for x64-based Systems Service Pack 2	Microsoft .NET Framework 4.6 (3189040)

	(Important)
Windows 7	
Bulletin Identifier	**MS16-120**
Aggregate Severity Rating	**Important**
Windows 7 for 32-bit Systems Service Pack 1	Microsoft .NET Framework 3.5.1 (3188730) (Important)
Windows 7 for x64-based Systems Service Pack 1	Microsoft .NET Framework 3.5.1 (3188730) (Important)
Windows Server 2008 R2	
Bulletin Identifier	**MS16-120**
Aggregate Severity Rating	**Important**
Windows Server 2008 R2 for x64-based Systems Service Pack 1	Microsoft .NET Framework 3.5.1 (3188730) (Important)
Windows Server 2008 R2 for Itanium-based Systems Service Pack 1	Microsoft .NET Framework 3.5.1 (3188730) (Important)
Windows 8.1	
Bulletin Identifier	**MS16-120**
Aggregate Severity Rating	**Important**
Windows 8.1 for 32-bit Systems	Microsoft .NET Framework 3.5 (3188732) (Important)
Windows 8.1 for x64-based Systems	Microsoft .NET Framework 3.5 (3188732) (Important)
Windows Server 2012 and Windows Server 2012 R2	
Bulletin Identifier	**MS16-120**
Aggregate Severity Rating	**Important**
Windows Server 2012	Microsoft .NET Framework 3.5 (3188731) (Important)
Windows Server 2012 R2	Microsoft .NET Framework 3.5 (3188732) (Important)
Windows 10	
Bulletin Identifier	**MS16-120**
Aggregate Severity Rating	**Important**

Windows 10 for 32-bit Systems (3192440)	Microsoft .NET Framework 3.5 (Important)
Windows 10 for x64-based Systems (3192440)	Microsoft .NET Framework 3.5 (Important)
Windows 10 Version 1511 for 32-bit Systems (3192441)	Microsoft .NET Framework 3.5 (Important)
Windows 10 Version 1511 for x64-based Systems (3192441)	Microsoft .NET Framework 3.5 (Important)
Windows 10 Version 1607 for 32-bit Systems (3194798)	Microsoft .NET Framework 3.5 (Important)
Windows 10 Version 1607 for x64-based Systems (3194798)	Microsoft .NET Framework 3.5 (Important)
Server Core installation option	
Bulletin Identifier	**MS16-120**
Aggregate Severity Rating	**Important**
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	Microsoft .NET Framework 3.5.1 (3188730) (Important)
Windows Server 2012 (Server Core installation)	Microsoft .NET Framework 3.5 (3188731) (Important)
Windows Server 2012 R2 (Server Core installation)	Microsoft .NET Framework 3.5 (3188732) (Important)

Microsoft .NET Framework – Monthly Rollup Release

Microsoft .NET Framework	
Windows Vista **Microsoft .NET Framework Updates for 3.0, 4.5.2 and 4.6 for Vista and Server 2008 (KB3188744)**	
Bulletin Identifier	**MS16-120**
Aggregate Severity Rating	**Important**
Windows Vista Service Pack 2	Microsoft .NET Framework 3.0 Service Pack 2 (3188735) Important
Windows Vista Service Pack 2	Microsoft .NET Framework 4.5.2 (3189051) Important
Windows Vista Service Pack 2	Microsoft .NET Framework 4.6 (3189052) Important
Windows Vista x64 Edition Service Pack 2	Microsoft .NET Framework 3.0 Service Pack 2

	(3188735) Important
Windows Vista x64 Edition Service Pack 2	Microsoft .NET Framework 4.5.2 (3189051) Important
Windows Vista x64 Edition Service Pack 2	Microsoft .NET Framework 4.6 (3189052) Important
Windows Server 2008 **Microsoft .NET Framework Updates for 3.0, 4.5.2 and 4.6 for Vista and Server 2008 (KB3188744)**	
Bulletin Identifier	**MS16-120**
Aggregate Severity Rating	**Important**
Windows Server 2008 for 32-bit Systems Service Pack 2	Microsoft .NET Framework 3.0 Service Pack 2 (3188735) Important
Windows Server 2008 for 32-bit Systems Service Pack 2	Microsoft .NET Framework 4.5.2 (3189051) Important
Windows Server 2008 for 32-bit Systems Service Pack 2	Microsoft .NET Framework 4.6 (3189052) Important
Windows Server 2008 for x64-based Systems Service Pack 2	Microsoft .NET Framework 3.0 Service Pack 2 (3188735) Important
Windows Server 2008 for x64-based Systems Service Pack 2	Microsoft .NET Framework 4.5.2 (3189051) Important
Windows Server 2008 for x64-based Systems Service Pack 2	Microsoft .NET Framework 4.6 (3189052) Important
Windows 7	
Bulletin Identifier	**MS16-120**
Aggregate Severity Rating	**Important**
Windows 7 for 32-bit Systems Service Pack 1	Microsoft .NET Framework 3.5.1 (3188740) Important
Windows 7 for x64-based Systems Service Pack 1	Microsoft .NET Framework 3.5.1 (3188740) Important
Windows Server 2008 R2	
Bulletin Identifier	**MS16-120**
Aggregate Severity Rating	**Important**
Windows Server 2008 R2 for x64-based Systems Service Pack 1	Microsoft .NET Framework 3.5.1 (3188740)

	Important
Windows Server 2008 R2 for Itanium-based Systems Service Pack 1	Microsoft .NET Framework 3.5.1 (3188740) Important
Windows 8.1	
Bulletin Identifier	**MS16-120**
Aggregate Severity Rating	**Important**
Windows 8.1 for 32-bit Systems	Microsoft .NET Framework 3.5 (3188743) Important
Windows 8.1 for x64-based Systems	Microsoft .NET Framework 3.5 (3188743) Important
Windows Server 2012 and Windows Server 2012 R2	
Bulletin Identifier	**MS16-120**
Aggregate Severity Rating	**Important**
Windows Server 2012	Microsoft .NET Framework 3.5 (3188741) Important
Windows Server 2012 R2	Microsoft .NET Framework 3.5 (3188743) Important
Windows 10	
Bulletin Identifier	**MS16-120**
Aggregate Severity Rating	**Important**
Windows 10 for 32-bit Systems (3192440)	Microsoft .NET Framework 3.5 Important
Windows 10 for x64-based Systems (3192440)	Microsoft .NET Framework 3.5 Important
Windows 10 Version 1511 for 32-bit Systems (3192441)	Microsoft .NET Framework 3.5 Important
Windows 10 Version 1511 for x64-based Systems (3192441)	Microsoft .NET Framework 3.5 Important
Windows 10 Version 1607 for 32-bit Systems (3194798)	Microsoft .NET Framework 3.5 Important
Windows 10 Version 1607 for x64-based Systems (3194798)	Microsoft .NET Framework 3.5 Important
Server Core installation option	
Bulletin Identifier	**MS16-120**
Aggregate Severity Rating	**Important**

Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	Microsoft .NET Framework 3.5.1 (3188740) Important
Windows Server 2012 (Server Core installation)	Microsoft .NET Framework 3.5 (3188741) Important
Windows Server 2012 R2 (Server Core installation)	Microsoft .NET Framework 3.5 (3188743) Important

Microsoft Communications Platforms and Software

Skype for Business 2016	
Bulletin Identifier	**MS16-120**
Aggregate Severity Rating	**Important**
Skype for Business 2016 (32-bit editions)	Skype for Business 2016 (32-bit editions) (3118327) (Important)
Skype for Business Basic 2016 (32-bit editions)	Skype for Business Basic 2016 (32-bit editions) (3118327) (Important)
Skype for Business 2016 (64-bit editions)	Skype for Business 2016 (64-bit editions) (3118327) (Important)
Skype for Business Basic 2016 (64-bit editions)	Skype for Business Basic 2016 (64-bit editions) (3118327) (Important)
Microsoft Lync 2013	
Bulletin Identifier	**MS16-120**
Aggregate Severity Rating	**Important**
Microsoft Lync 2013 Service Pack 1 (32-bit) (Skype for Business)	Microsoft Lync 2013 Service Pack 1 (32-bit) (Skype for Business) (3118348) (Important)
Microsoft Lync Basic 2013 Service Pack 1 (32-bit) (Skype for Business Basic)	Microsoft Lync Basic 2013 Service Pack 1 (32-bit) (Skype for Business Basic) (3118348) (Important)
Microsoft Lync 2013 Service Pack 1 (64-bit) (Skype for Business)	Microsoft Lync 2013 Service Pack 1 (64-bit) (Skype for Business) (3118348) (Important)
Microsoft Lync Basic 2013 Service Pack 1 (64-bit) (Skype for Business Basic)	Microsoft Lync Basic 2013 Service Pack 1 (64-bit) (Skype for Business Basic)

	(3118348) (Important)
Microsoft Lync 2010	
Bulletin Identifier	**MS16-120**
Aggregate Severity Rating	**Important**
Microsoft Lync 2010 (32-bit)	Microsoft Lync 2010 (32-bit) (3188397) (Important)
Microsoft Lync 2010 (64-bit)	Microsoft Lync 2010 (64-bit) (3188397) (Important)
Microsoft Lync 2010 Attendee (user level install)	Microsoft Lync 2010 Attendee (user level install) (3188399) (Important)
Microsoft Lync 2010 Attendee (admin level install)	Microsoft Lync 2010 Attendee (admin level install) (3188400) (Important)
Microsoft Live Meeting 2007 Console	
Bulletin Identifier	**MS16-120**
Aggregate Severity Rating	**Important**
Microsoft Live Meeting 2007 Console	Microsoft Live Meeting 2007 Console (3189647) (Important)

Microsoft Developer Tools and Software

Microsoft Silverlight	
Bulletin Identifier	**MS16-120**
Aggregate Severity Rating	**Important**
Microsoft Silverlight 5 when installed on Mac	Microsoft Silverlight 5 when installed on Mac (3193713) **(**Important)
Microsoft Silverlight 5 Developer Runtime when installed on Mac	Microsoft Silverlight 5 Developer Runtime when installed on Mac (3193713) **(**Important)
Microsoft Silverlight 5 when installed on all supported releases of Microsoft Windows clients	Microsoft Silverlight 5 when installed on all supported releases of Microsoft Windows clients (3193713) **(**Important)
Microsoft Silverlight 5 Developer Runtime when installed on all supported releases of Microsoft Windows clients	Microsoft Silverlight 5 Developer Runtime when installed on all supported releases of Microsoft Windows clients

	(3193713) **(**Important)
Microsoft Silverlight 5 when installed on all supported releases of Microsoft Windows servers	Microsoft Silverlight 5 when installed on all supported releases of Microsoft Windows servers (3193713) **(**Important)
Microsoft Silverlight 5 Developer Runtime when installed on all supported releases of Microsoft Windows servers	Microsoft Silverlight 5 Developer Runtime when installed on all supported releases of Microsoft Windows servers (3193713) **(**Important)

Microsoft Office Suites and Software

Microsoft Office 2007		
Bulletin Identifier	**MS16-120**	**MS16-121**
Aggregate Severity Rating	**Important**	**Critical**
Microsoft Office 2007 Service Pack 3	Microsoft Office 2007 Service Pack 3 (3118301) (Important)	Microsoft Word 2007 Service Pack 3 (3118308) (Critical)
Microsoft Office 2010		
Bulletin Identifier	**MS16-120**	**MS16-121**
Aggregate Severity Rating	**Important**	**Critical**
Microsoft Office 2010 Service Pack 2 (32-bit editions)	Microsoft Office 2010 Service Pack 2 (32-bit editions) (3118317) (Important)	Microsoft Office 2010 Service Pack 2 (32-bit editions) (3118311) (Critical) Microsoft Word 2010 Service Pack 2 (32-bit editions) (3118312) (Critical)
Microsoft Office 2010 Service Pack 2 (64-bit editions)	Microsoft Office 2010 Service Pack 2 (64-bit editions) (3118317) (Important)	Microsoft Office 2010 Service Pack 2 (64-bit editions) (3118311) (Critical) Microsoft Word 2010 Service Pack 2 (64-bit editions) (3118312) (Critical)
Microsoft Office 2013		
Bulletin Identifier	**MS16-120**	**MS16-121**
Aggregate Severity Rating	**None**	**Critical**
Microsoft Office 2013 Service Pack 1 (32-bit editions)	Not applicable	Microsoft Word 2013 Service Pack 1 (32-bit editions) (3118345) (Critical)

Microsoft Office 2013 Service Pack 1 (64-bit editions)	Not applicable	Microsoft Word 2013 Service Pack 1 (64-bit editions) (3118345) (Critical)
Microsoft Office 2013 RT		
Bulletin Identifier	**MS16-120**	**MS16-121**
Aggregate Severity Rating	**None**	**Critical**
Microsoft Office 2013 RT Service Pack 1	Not applicable	Microsoft Word 2013 RT Service Pack 1 (3118345) (Critical)
Microsoft Office 2016		
Bulletin Identifier	**MS16-120**	**MS16-121**
Aggregate Severity Rating	**None**	**Critical**
Microsoft Office 2016 (32-bit edition)	Not applicable	Microsoft Word 2016 (32-bit edition) (3118331) (Critical)
Microsoft Office 2016 (64-bit edition)	Not applicable	Microsoft Word 2016 (64-bit edition) (3118331) (Critical)
Microsoft Office for Mac 2011		
Bulletin Identifier	**MS16-120**	**MS16-121**
Aggregate Severity Rating	**None**	**Critical**
Microsoft Office for Mac 2011	Not applicable	Microsoft Word for Mac 2011 (3193442) (Critical)
Microsoft Office 2016 for Mac		
Bulletin Identifier	**MS16-120**	**MS16-121**
Aggregate Severity Rating	**None**	**Critical**
Microsoft Office 2016 for Mac	Not applicable	Microsoft Word 2016 for Mac (3193438) (Critical)
Other Office Software		
Bulletin Identifier	**MS16-120**	**MS16-121**
Aggregate Severity Rating	**Important**	**Critical**
Microsoft Office Compatibility Pack Service Pack 3	Not applicable	Microsoft Office Compatibility Pack Service Pack 3 (3118307) (Critical)
Microsoft Word Viewer	Microsoft Word Viewer (3118394)	Microsoft Word Viewer (3127898)

	(Important)	(Critical)

Microsoft Office Services and Web Apps

Microsoft SharePoint Server 2010	
Bulletin Identifier	**MS16-121**
Aggregate Severity Rating	**Critical**
Microsoft SharePoint Server 2010 Service Pack 2	Word Automation Services (3118377) (Critical)
Microsoft SharePoint Server 2013	
Bulletin Identifier	**MS16-121**
Aggregate Severity Rating	**Critical**
Microsoft SharePoint Server 2013 Service Pack 1	Word Automation Services (3118352) (Critical)
Microsoft Office Web Apps 2010	
Bulletin Identifier	**MS16-121**
Aggregate Severity Rating	**Critical**
Microsoft Office Web Apps 2010 Service Pack 2	Microsoft Office Web Apps 2010 Service Pack 2 (3118384) (Critical)
Microsoft Office Web Apps 2013	
Bulletin Identifier	**MS16-121**
Aggregate Severity Rating	**Critical**
Microsoft Office Web Apps Server 2013 Service Pack 1	Microsoft Office Web Apps Server 2013 Service Pack 1 (3118360) (Critical)
Office Online Server	Office Online Server (3127897) (Critical)

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 (October 11, 2016): Bulletin Summary published.
- V1.1 (October 12, 2016): Bulletin Summary revised to change the severity of MS16-121 to Critical. This is an informational change only.
- V2.0 (October 27, 2016): Bulletin Summary revised added a new bulletin for Flash MS16-128.
- V3.0 (September 12, 2017): For MS16-123, revised the Windows Operating System and Components affected software table to include Windows 10 Version 1703 for 32-bit Systems and Windows 10 Version 1703 for x64-based Systems because they are affected by CVE-2016-3376. Consumers using Windows 10 are automatically protected. Microsoft recommends that enterprise customers running Windows 10 Version 1703 ensure they have update 4038788 installed to be protected from this vulnerability.

Page generated 2017-09-09 17:48-07:00.