Microsoft Security Bulletin Summary for September 2016

Published: September 13, 2016 | Updated: July 11, 2017

Version: 2.0

This bulletin summary lists security bulletins released for September 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

Exploitability Index

Affected Software

Detection and Deployment Tools and Guidance

Acknowledgments

Other Information

Executive Summaries

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

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

Bulletin ID	Bulletin Title and Executive Summary	Maximum Severity Rating and Vulnerability Impact	Restart Requirement	Known Issues	Affected Software
MS16-104	**Cumulative Security Update for Internet Explorer (3183038)** 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	3185319	Microsoft Windows, Internet Explorer
MS16-105	**Cumulative Security Update for Microsoft Edge (3183043)** 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	---------	Microsoft Windows, Microsoft Edge

MS16-106	**Security Update for Microsoft Graphics Component (3185848)** 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
MS16-107	**Security Update for Microsoft Office (3185852)** 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
MS16-108	**Security Update for Microsoft Exchange Server (3185883)** This security update resolves vulnerabilities in Microsoft Exchange Server. The most severe of the vulnerabilities could allow remote code execution in some Oracle Outside In libraries that are built into Exchange Server if an attacker sends an email with a specially crafted attachment to a vulnerable Exchange server.	Critical Remote Code Execution	May require restart	---------	Microsoft Exchange
MS16-109	**Security Update for Silverlight (3182373)** This security update resolves a vulnerability in Microsoft Silverlight. The vulnerability could allow remote code execution if a user visits a compromised website that contains a specially crafted Silverlight application. An attacker would have no way to force a user to visit a compromised website. Instead, an attacker would have to convince the user to visit the website, typically by enticing the user to click a link in either an email or instant message that takes the user to the attacker's website.	Important Remote Code Execution	Does not require restart	---------	Microsoft Windows
MS16-110	**Security Update for Windows (3178467)** This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker creates a specially crafted request and executes arbitrary code with elevated permissions on a target system.	Important Remote Code Execution	Requires restart	3187754	Microsoft Windows
MS16-111	**Security Update for Windows Kernel (3186973)** This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities	Important Elevation of Privilege	Requires restart	3175024	Microsoft Windows

	could allow elevation of privilege if an attacker runs a specially crafted application on a target system.				
MS16-112	**Security Update for Windows Lock Screen (3178469)** This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if Windows improperly allows web content to load from the Windows lock screen.	Important Elevation of Privilege	Requires restart	---------	Microsoft Windows
MS16-113	**Security Update for Windows Secure Kernel Mode (3185876)** This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow information disclosure when Windows Secure Kernel Mode improperly handles objects in memory.	Important Information Disclosure	Requires restart	---------	Microsoft Windows
MS16-114	**Security Update for SMBv1 Server (3185879)** This security update resolves a vulnerability in Microsoft Windows. On Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2 operating systems, the vulnerability could allow remote code execution if an authenticated attacker sends specially crafted packets to an affected Microsoft Server Message Block 1.0 (SMBv1) Server. The vulnerability does not impact other SMB Server versions. Although later operating systems are affected, the potential impact is denial of service.	Important Remote Code Execution	Requires restart	---------	Microsoft Windows
MS16-115	**Security Update for Microsoft Windows PDF Library (3188733)** This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities could allow information disclosure if a user views specially crafted PDF content online or opens a specially crafted PDF document.	Important Information Disclosure	May require restart	---------	Microsoft Windows
MS16-116	**Security Update in OLE Automation for VBScript Scripting Engine (3188724)** This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if an attacker successfully convinces a user of an affected system to visit a malicious or compromised website. Note that you must install two updates to be protected from the vulnerability discussed in this bulletin: The update in this bulletin, MS16-116, and the update in MS16-104.	Critical Remote Code Execution	Requires restart	---------	Microsoft Windows
MS16-117	**Security Update for Adobe Flash Player (3188128)** 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
MS16-104: Cumulative Security Update for Internet Explorer (3183038)				
CVE-2016-3247	Microsoft Browser Memory Corruption Vulnerability	2 - Exploitation Less Likely	4 - Not affected	Not applicable
CVE-2016-3291	Microsoft Browser Information Disclosure Vulnerability	3 - Exploitation Unlikely	4 - Not affected	Not applicable
CVE-2016-3292	Microsoft Browser Elevation of Privilege Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-3295	Microsoft Browser Memory Corruption Vulnerability	3 - Exploitation Unlikely	3 - Exploitation Unlikely	Not applicable
CVE-2016-3297	Microsoft Browser Memory Corruption Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2016-3324	Internet Explorer Memory Corruption Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2016-3325	Microsoft Browser Information Disclosure Vulnerability	2 - Exploitation Less Likely	4 - Not affected	Not applicable
CVE-2016-3351	Microsoft Browser Information Disclosure Vulnerability	0 - Exploitation Detected	0 - Exploitation Detected	Not applicable
CVE-2016-3353	Internet Explorer Security Feature Bypass	3- Exploitation Unlikely	3- Exploitation Unlikely	Not applicable

CVE-2016-3375	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
MS16-105: Cumulative Security Update for Microsoft Edge (3183043)				
CVE-2016-3247	Microsoft Browser Memory Corruption Vulnerability	2 - Exploitation Less Likely	4 - Not affected	Not applicable
CVE-2016-3291	Microsoft Browser Information Disclosure Vulnerability	3 - Exploitation Unlikely	4 - Not affected	Not applicable
CVE-2016-3294	Microsoft Edge Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-3295	Microsoft Browser Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-3297	Microsoft Browser Memory Corruption Vulnerability	2 - Exploitation Less Likely	4 - Not affected	Not applicable
CVE-2016-3325	Microsoft Browser Information Disclosure Vulnerability	2 - Exploitation Less Likely	4 - Not affected	Not applicable
CVE-2016-3330	Microsoft Edge Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-3350	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-3351	Microsoft Browser Information Disclosure Vulnerability	0 - Exploitation Detected	4 - Not affected	Not applicable
CVE-2016-3370	PDF Library Information Disclosure Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-3374	PDF Library Information Disclosure Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-3377	Scripting Engine Memory	1 - Exploitation More Likely	4 - Not affected	Not applicable

	Corruption Vulnerability			
MS16-106: Security Update for Microsoft Graphics Component (3185848)				
CVE-2016-3348	Win32k Elevation of Privilege Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-3349	Win32k Elevation of Privilege Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE–2016-3354	GDI Information Disclosure Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE–2016-3355	GDI Elevation of Privilege Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE–2016-3356	GDI Remote Code Execution Vulnerability	2 - Exploitation Less Likely	4 - Not affected	Not applicable
MS16-107: Security Update for Microsoft Office (3185852)				
CVE-2016-0137	Microsoft APP-V ASLR Bypass	2 - Exploitation Less Likely	4 - Not affected	Not applicable
CVE-2016-0141	Microsoft Information Disclosure Vulnerability	3 - Exploitation Unlikely	3 - Exploitation Unlikely	Not applicable
CVE-2016-3357	Microsoft Office Memory Corruption Vulnerability	4 - Not affected	2 - Exploitation Less Likely	Not applicable
CVE-2016-3358	Microsoft Office Memory Corruption Vulnerability	4 - Not affected	2 - Exploitation Less Likely	Not applicable
CVE-2016-3359	Microsoft Office Memory Corruption Vulnerability	4 - Not affected	2 - Exploitation Less Likely	Not applicable
CVE-2016-3360	Microsoft Office Memory Corruption Vulnerability	4 - Not affected	2 - Exploitation Less Likely	Not applicable
CVE-2016-3361	Microsoft Office Memory Corruption Vulnerability	4 - Not affected	2 - Exploitation Less Likely	Not applicable
CVE-2016-3362	Microsoft Office Memory Corruption Vulnerability	4 - Not affected	2 - Exploitation Less Likely	Not applicable

CVE-2016-3363	Microsoft Office Memory Corruption Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2016-3364	Microsoft Office Memory Corruption Vulnerability	2 - Exploitation Less Likely	4 - Not affected	Not applicable
CVE-2016-3365	Microsoft Office Memory Corruption Vulnerability	4 - Not affected	2 - Exploitation Less Likely	Not applicable
CVE-2016-3366	Microsoft Office Spoofing Vulnerability	3 - Exploitation Unlikely	3 - Exploitation Unlikely	Not applicable
CVE-2016-3381	Microsoft Office Memory Corruption Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
MS16-108: Security Update for Microsoft Exchange Server (3185883)				
CVE-2016-0138	Microsoft Exchange Information Disclosure Vulnerability	3 - Exploitation Unlikely	3 - Exploitation Unlikely	Not applicable
CVE-2016-3378	Microsoft Exchange Open Redirect Vulnerability	3 - Exploitation Unlikely	3 - Exploitation Unlikely	Not applicable
CVE-2016-3379	Microsoft Exchange Elevation of Privilege Vulnerability	2 - Exploitation Less Likely	4 - Not affected	Not applicable
MS16-109: Security Update for Silverlight (3182373)				
CVE-2016-3367	Microsoft Silverlight Memory Corruption Vulnerability	3 - Exploitation Unlikely	3 - Exploitation Unlikely	Not applicable
MS16-110: Security Update for Windows (3178467)				
CVE-2016-3346	Windows Permissions Enforcement Elevation of Privilege Vulnerability	2 - Exploitation Less Likely	4 - Not affected	Not applicable
CVE-2016-3352	Microsoft Information Disclosure Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-3368	Windows Remote	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable

	Code Execution Vulnerability			
CVE-2016-3369	Windows Denial of Service Vulnerability	3 - Exploitation Unlikely	4 - Not affected	Permanent
MS16-111: Security Update for Windows Kernel (3186973)				
CVE-2016-3305	Windows Session Object Elevation of Privilege Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2016-3306	Windows Session Object Elevation of Privilege Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2016-3371	Windows Kernel Elevation of Privilege Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2016-3372	Windows Kernel Elevation of Privilege Vulnerability	4 - Not affected	3 - Exploitation Unlikely	Not applicable
CVE-2016-3373	Windows Kernel Elevation of Privilege Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
MS16-112: Security Update for Lock Screen (3178469)				
CVE-2016-3302	Windows Lock Screen Elevation of Privilege Vulnerability	3 - Exploitation Unlikely	3 - Exploitation Unlikely	Not applicable
MS16-113: Security Update for Windows Secure Kernel Mode (3185876)				
CVE-2016-3344	Windows Secure Kernel Mode Information Disclosure Vulnerability	3 - Exploitation Unlikely	4 - Not affected	Not applicable
MS16-114: Security Update for SMBv1 Server (3185879)				
CVE-2016-3345	Windows SMB Authenticated Remote Code Execution Vulnerability	3 - Exploitation Unlikely	3 - Exploitation Unlikely	Permanent
MS16-115: Security Update for Microsoft Windows PDF Library (3188733)				
CVE-2016-3370	PDF Library Information Disclosure Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable

CVE-2016-3374	PDF Library Information Disclosure Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
MS16-116: Security Update in OLE Automation for VBScript Scripting Engine (3188724)				
CVE-2016-3375	Scripting Engine Information Disclosure Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
MS16-117: Security Update for Adobe Flash Player (3188128)				
APSB16-29	See Adobe Security Bulletin APSB16-29 for vulnerability severity and update priority ratings.	Not applicable	Not applicable	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	**MS16-104**	**MS16-105**	**MS16-106**	**MS16-110**	**MS16-111**	**MS16-112**
Aggregate Severity Rating	**Critical**	**None**	**Important**	**Important**	**Important**	**None**
Windows Vista Service Pack 2	Internet Explorer 9 (3185319) (Critical)	Not applicable	Windows Vista Service Pack 2 (3185911) (Important)	Windows Vista Service Pack 2 (3184471) (Important)	Windows Vista Service Pack 2 (3175024) (Important)	Not applicable
Windows Vista x64 Edition Service Pack 2	Internet Explorer 9 (3185319) (Critical)	Not applicable	Windows Vista x64 Edition Service Pack 2 (3185911) (Important)	Windows Vista x64 Edition Service Pack 2 (3184471) (Important)	Windows Vista x64 Edition Service Pack 2 (3175024) (Important)	Not applicable
Windows Server 2008						
Bulletin	**MS16-104**	**MS16-105**	**MS16-106**	**MS16-110**	**MS16-111**	**MS16-112**

Identifier						
Aggregate Severity Rating	**Moderate**	**None**	**Important**	**Important**	**Important**	**None**
Windows Server 2008 for 32-bit Systems Service Pack 2	Internet Explorer 9 (3185319) (Moderate)	Not applicable	Windows Server 2008 for 32-bit Systems Service Pack 2 (3185911) (Important)	Windows Server 2008 for 32-bit Systems Service Pack 2 (3184471) (Important)	Windows Server 2008 for 32-bit Systems Service Pack 2 (3175024) (Important)	Not applicable
Windows Server 2008 for x64-based Systems Service Pack 2	Internet Explorer 9 (3185319) (Moderate)	Not applicable	Windows Server 2008 for x64-based Systems Service Pack 2 (3185911) (Important)	Windows Server 2008 for x64-based Systems Service Pack 2 (3184471) (Important)	Windows Server 2008 for x64-based Systems Service Pack 2 (3175024) (Important)	Not applicable
Windows Server 2008 for Itanium-based Systems Service Pack 2	Not applicable	Not applicable	Windows Server 2008 for Itanium-based Systems Service Pack 2 (3185911) (Important)	Not applicable	Windows Server 2008 for Itanium-based Systems Service Pack 2 (3175024) (Important)	Not applicable
Windows 7						
Bulletin Identifier	**MS16-104**	**MS16-105**	**MS16-106**	**MS16-110**	**MS16-111**	**MS16-112**
Aggregate Severity Rating	**Critical**	**None**	**Important**	**Important**	**Important**	**None**
Windows 7 for 32-bit Systems Service Pack 1	Internet Explorer 11 (3185319) (Critical)	Not applicable	Windows 7 for 32-bit Systems Service Pack 1 (3185911) (Important)	Windows 7 for 32-bit Systems Service Pack 1 (3184471) (Important)	Windows 7 for 32-bit Systems Service Pack 1 (3175024) (Important)	Not applicable
Windows 7 for x64-based Systems Service Pack 1	Internet Explorer 11 (3185319) (Critical)	Not applicable	Windows 7 for x64-based Systems Service Pack 1 (3185911) (Important)	Windows 7 for x64-based Systems Service Pack 1 (3184471) (Important)	Windows 7 for x64-based Systems Service Pack 1 (3175024) (Important)	Not applicable
Windows Server 2008 R2						
Bulletin Identifier	**MS16-104**	**MS16-105**	**MS16-106**	**MS16-110**	**MS16-111**	**MS16-112**
Aggregate Severity Rating	**Moderate**	**None**	**Important**	**Important**	**Important**	**None**
Windows Server 2008 R2	Internet Explorer 11 (3185319)	Not applicable	Windows Server 2008 R2	Windows Server 2008 R2	Windows Server 2008	Not applicable

for x64-based Systems Service Pack 1	(Moderate)		for x64-based Systems Service Pack 1 (3185911) (Important)	for x64-based Systems Service Pack 1 (3184471) (Important)	R2 for x64-based Systems Service Pack 1 (3175024) (Important)	
Windows Server 2008 R2 for Itanium-based Systems Service Pack 1	Not applicable	Not applicable	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3185911) (Important)	Not applicable	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3175024) (Important)	Not applicable
Windows 8.1						
Bulletin Identifier	**MS16-104**	**MS16-105**	**MS16-106**	**MS16-110**	**MS16-111**	**MS16-112**
Aggregate Severity Rating	**Critical**	**None**	**Important**	**Important**	**Important**	**Important**
Windows 8.1 for 32-bit Systems	Internet Explorer 11 (3185319) (Critical)	Not applicable	Windows 8.1 for 32-bit Systems (3185911) (Important)	Windows 8.1 for 32-bit Systems (3184471) (Important) Windows 8.1 for 32-bit Systems (3187754) (Important)	Windows 8.1 for 32-bit Systems (3175024) (Important)	Windows 8.1 for 32-bit Systems (3178539) (Important)
Windows 8.1 for x64-based Systems	Internet Explorer 11 (3185319) (Critical)	Not applicable	Windows 8.1 for x64-based Systems (3185911) (Important)	Windows 8.1 for x64-based Systems (3184471) (Important) Windows 8.1 for x64-based Systems (3187754) (Important)	Windows 8.1 for x64-based Systems (3175024) (Important)	Windows 8.1 for x64-based Systems (3178539) (Important)
Windows Server 2012 and Windows Server 2012 R2						
Bulletin Identifier	**MS16-104**	**MS16-105**	**MS16-106**	**MS16-110**	**MS16-111**	**MS16-112**
Aggregate Severity Rating	**Moderate**	**None**	**Important**	**Important**	**Important**	**Important**
Windows Server 2012	Internet Explorer 10 (3185319) (Moderate)	Not applicable	Windows Server 2012 (3185911) (Important)	Windows Server 2012 (3184471) (Important)	Windows Server 2012 (3175024) (Important)	Not applicable
Windows	Internet Explorer 11	Not applicable	Windows	Windows	Windows	Windows

Server 2012 R2	(3185319) (Moderate)		Server 2012 R2 (3185911) (Important)	Server 2012 R2 (3184471) (Important)	Server 2012 R2 (3175024) (Important)	Server 2012 R2 (3178539) (Important)
Windows RT 8.1						
Bulletin Identifier	**MS16-104**	**MS16-105**	**MS16-106**	**MS16-110**	**MS16-111**	**MS16-112**
Aggregate Severity Rating	**Critical**	**None**	**Important**	**Important**	**Important**	**Important**
Windows RT 8.1	Internet Explorer 11 (3185319) (Critical)	Not applicable	Windows RT 8.1 (3185911) (Important)	Windows RT 8.1 (3184471) (Important) Windows RT 8.1 (3187754) (Important)	Windows RT 8.1 (3175024) (Important)	Windows RT 8.1 (3178539) (Important)
Windows 10						
Bulletin Identifier	**MS16-104**	**MS16-105**	**MS16-106**	**MS16-110**	**MS16-111**	**MS16-112**
Aggregate Severity Rating	**Critical**	**Critical**	**Critical**	**Important**	**Important**	**Important**
Windows 10 for 32-bit Systems	Internet Explorer 11 (3185611) (Critical)	Microsoft Edge (3185611) (Critical)	Windows 10 for 32-bit Systems (3185611) (Important)	Windows 10 for 32-bit Systems (3185611) (Important)	Windows 10 for 32-bit Systems (3185611) (Important)	Windows 10 for 32-bit Systems (3185611) (Important)
Windows 10 for x64-based Systems	Internet Explorer 11 (3185611) (Critical)	Microsoft Edge (3185611) (Critical)	Windows 10 for x64-based Systems (3185611) (Important)	Windows 10 for x64-based Systems (3185611) (Important)	Windows 10 for x64-based Systems (3185611) (Important)	Windows 10 for x64-based Systems (3185611) (Important)
Windows 10 Version 1511 for 32-bit Systems	Internet Explorer 11 (3185614) (Critical)	Microsoft Edge (3185614) (Critical)	Windows 10 Version 1511 for 32-bit Systems (3185614) (Important)	Windows 10 Version 1511 for 32-bit Systems (3185614) (Important)	Windows 10 Version 1511 for 32-bit Systems (3185614) (Important)	Windows 10 Version 1511 for 32-bit Systems (3185614) (Important)
Windows 10 Version 1511 for x64-based Systems	Internet Explorer 11 (3185614) (Critical)	Microsoft Edge (3185614) (Critical)	Windows 10 Version 1511 for x64-based Systems (3185614) (Important)	Windows 10 Version 1511 for x64-based Systems (3185614) (Important)	Windows 10 Version 1511 for x64-based Systems (3185614) (Important)	Windows 10 Version 1511 for x64-based Systems (3185614) (Important)
Windows 10 Version 1607 for 32-bit Systems	Internet Explorer 11 (3189866) (Critical)	Microsoft Edge (3189866) (Critical)	Windows 10 Version 1607 for 32-bit Systems (3189866) (Critical)	Windows 10 Version 1607 for 32-bit Systems (3189866) (Important)	Windows 10 Version 1607 for 32-bit Systems (3189866) (Important)	Windows 10 Version 1607 for 32-bit Systems (3189866) (Important)

Windows 10 Version 1607 for x64-based Systems	Internet Explorer 11 (3189866) (Critical)	Microsoft Edge (3189866) (Critical)	Windows 10 Version 1607 for x64-based Systems (3189866) (Critical)	Windows 10 Version 1607 for x64-based Systems (3189866) (Important)	Windows 10 Version 1607 for x64-based Systems (3189866) (Important)	Windows 10 Version 1607 for 32-bit Systems (3189866) (Important)
Windows 10 Version 1703 for 32-bit Systems	Not applicable	Not applicable	Not applicable	Not applicable	Windows 10 Version 1703 for 32-bit Systems (4025342) (Important)	Not applicable
Windows 10 Version 1703 for x64-based Systems	Not applicable	Not applicable	Not applicable	Not applicable	Windows 10 Version 1703 for x64-based Systems (4025342) (Important)	Not applicable
Server Core installation option						
Bulletin Identifier	**MS16-104**	**MS16-105**	**MS16-106**	**MS16-110**	**MS16-111**	**MS16-112**
Aggregate Severity Rating	**None**	**None**	**Important**	**Important**	**Important**	**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) (3185911) (Important)	Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (3184471) (Important)	Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (3175024) (Important)	Not applicable
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) (3185911) (Important)	Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) (3184471) (Important)	Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) (3175024) (Important)	Not applicable
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	Not applicable	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3185911) (Important)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3184471) (Important)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3175024) (Important)	Not applicable
Windows Server 2012 (Server Core installation)	Not applicable	Not applicable	Windows Server 2012 (Server Core installation)	Windows Server 2012 (Server Core installation)	Windows Server 2012 (Server Core installation)	Not applicable

			(3185911) (Important)	(3184471) (Important)	(3175024) (Important)	
Windows Server 2012 R2 (Server Core installation)	Not applicable	Not applicable	Windows Server 2012 R2 (Server Core installation) (3185911) (Important)	Windows Server 2012 R2 (Server Core installation) (3184471) (Important)	Windows Server 2012 R2 (Server Core installation) (3175024) (Important)	Windows Server 2012 R2 (Server Core installation) (3178539) (Important)

Windows Operating Systems and Components (Table 2 of 2)

Windows Vista					
Bulletin Identifier	**MS16-113**	**MS16-114**	**MS16-115**	**MS16-116**	**MS16-117**
Aggregate Severity Rating	**None**	**Important**	**None**	**Critical**	**None**
Windows Vista Service Pack 2	Not applicable	Windows Vista Service Pack 2 (3177186) (Important)	Not applicable	Windows Vista Service Pack 2 (3184122) (Critical)	Not applicable
Windows Vista x64 Edition Service Pack 2	Not applicable	Windows Vista x64 Edition Service Pack 2 (3177186) (Important)	Not applicable	Windows Vista x64 Edition Service Pack 2 (3184122) (Critical)	Not applicable
Windows Server 2008					
Bulletin Identifier	**MS16-113**	**MS16-114**	**MS16-115**	**MS16-116**	**MS16-117**
Aggregate Severity Rating	**None**	**Important**	**None**	**Moderate**	**None**
Windows Server 2008 for 32-bit Systems Service Pack 2	Not applicable	Windows Server 2008 for 32-bit Systems Service Pack 2 (3177186) (Important)	Not applicable	Windows Server 2008 for 32-bit Systems Service Pack 2 (3184122) (Moderate)	Not applicable
Windows Server 2008 for x64-based Systems Service Pack 2	Not applicable	Windows Server 2008 for x64-based Systems Service Pack 2 (3177186) (Important)	Not applicable	Windows Server 2008 for x64-based Systems Service Pack 2 (3184122) (Moderate)	Not applicable
Windows Server 2008 for Itanium-based Systems Service Pack 2	Not applicable	Windows Server 2008 for Itanium-based Systems Service Pack 2 (3177186) (Important)	Not applicable	Windows Server 2008 for Itanium-based Systems Service Pack 2 (3184122) (Moderate)	Not applicable
Windows 7					
Bulletin Identifier	**MS16-113**	**MS16-114**	**MS16-115**	**MS16-116**	**MS16-117**
Aggregate Severity Rating	**None**	**Important**	**None**	**Critical**	**None**

Windows 7 for 32-bit Systems Service Pack 1	Not applicable	Windows 7 for 32-bit Systems Service Pack 1 (3177186) (Important)	Not applicable	Windows 7 for 32-bit Systems Service Pack 1 (3184122) (Critical)	Not applicable
Windows 7 for x64-based Systems Service Pack 1	Not applicable	Windows 7 for x64-based Systems Service Pack 1 (3177186) (Important)	Not applicable	Windows 7 for x64-based Systems Service Pack 1 (3184122) (Critical)	Not applicable
Windows Server 2008 R2					
Bulletin Identifier	**MS16-113**	**MS16-114**	**MS16-115**	**MS16-116**	**MS16-117**
Aggregate Severity Rating	**None**	**Important**	**None**	**Moderate**	**None**
Windows Server 2008 R2 for x64-based Systems Service Pack 1	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3177186) (Important)	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3184122) (Moderate)	Not applicable
Windows Server 2008 R2 for Itanium-based Systems Service Pack 1	Not applicable	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3177186) (Important)	Not applicable	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3184122) (Moderate)	Not applicable
Windows 8.1					
Bulletin Identifier	**MS16-113**	**MS16-114**	**MS16-115**	**MS16-116**	**MS16-117**
Aggregate Severity Rating	**None**	**Important**	**Important**	**Critical**	**Critical**
Windows 8.1 for 32-bit Systems	Not applicable	Windows 8.1 for 32-bit Systems (3177186) (Important)	Windows 8.1 for 32-bit Systems (3184943) (Important)	Windows 8.1 for 32-bit Systems (3184122) (Critical)	Windows 8.1 for 32-bit Systems (3188128) (Critical)
Windows 8.1 for x64-based Systems	Not applicable	Windows 8.1 for x64-based Systems (3177186) (Important)	Windows 8.1 for x64-based Systems (3184943) (Important)	Windows 8.1 for x64-based Systems (3184122) (Critical)	Windows 8.1 for x64-based Systems (3188128) (Critical)
Windows Server 2012 and Windows Server 2012 R2					
Bulletin Identifier	**MS16-113**	**MS16-114**	**MS16-115**	**MS16-116**	**MS16-117**
Aggregate Severity Rating	**None**	**Important**	**Important**	**Moderate**	**Moderate**
Windows Server 2012	Not applicable	Windows Server 2012 (3177186) (Important)	Windows Server 2012 (3184943) (Important)	Windows Server 2012 (3184122) (Moderate)	Windows Server 2012 (3188128) (Moderate)
Windows Server 2012 R2	Not applicable	Windows Server 2012 R2 (3177186) (Important)	Windows Server 2012 R2	Windows Server 2012 R2 (3184122) (Moderate)	Windows Server 2012 R2

			(3184943) (Important)		(3188128) (Moderate)
Windows RT 8.1					
Bulletin Identifier	**MS16-113**	**MS16-114**	**MS16-115**	**MS16-116**	**MS16-117**
Aggregate Severity Rating	**None**	**Important**	**Important**	**Critical**	**Critical**
Windows RT 8.1	Not applicable	Windows RT 8.1 (3177186) (Important)	Windows RT 8.1 (3184943) (Important)	Windows RT 8.1 (3184122) (Critical)	Windows RT 8.1 (3188128) (Critical)
Windows 10					
Bulletin Identifier	**MS16-113**	**MS16-114**	**MS16-115**	**MS16-116**	**MS16-117**
Aggregate Severity Rating	**Important**	**Important**	**Important**	**Critical**	**Critical**
Windows 10 for 32-bit Systems	Windows 10 for 32-bit Systems (3185611) (Important)	Windows 10 for 32-bit Systems (3185611) (Important)	Windows 10 for 32-bit Systems (3185611) (Important)	Windows 10 for 32-bit Systems (3185611) (Critical)	Windows 10 for 32-bit Systems (3188128) (Critical)
Windows 10 for x64-based Systems	Windows 10 for x64-based Systems (3185611) (Important)	Windows 10 for x64-based Systems (3185611) (Important)	Windows 10 for x64-based Systems (3185611) (Important)	Windows 10 for x64-based Systems (3185611) (Critical)	Windows 10 for x64-based Systems (3188128) (Critical)
Windows 10 Version 1511 for 32-bit Systems	Windows 10 Version 1511 for 32-bit Systems (3185614) (Important)	Windows 10 Version 1511 for 32-bit Systems (3185614) (Important)	Windows 10 Version 1511 for 32-bit Systems (3185614) (Important)	Windows 10 Version 1511 for 32-bit Systems (3185614) (Critical)	Windows 10 Version 1511 for 32-bit Systems (3188128) (Critical)
Windows 10 Version 1511 for x64-based Systems	Windows 10 Version 1511 for x64-based Systems (3185614) (Important)	Windows 10 Version 1511 for x64-based Systems (3185614) (Important)	Windows 10 Version 1511 for x64-based Systems (3185614) (Important)	Windows 10 Version 1511 for x64-based Systems (3185614) (Critical)	Windows 10 Version 1511 for x64-based Systems (3188128) (Critical)
Windows 10 Version 1607 for 32-bit Systems	Not applicable	Windows 10 Version 1607 for 32-bit Systems (3185614) (Important)	Windows 10 Version 1607 for 32-bit Systems (3189866) (Important)	Windows 10 Version 1607 for 32-bit Systems (3189866) (Critical)	Windows 10 Version 1607 for 32-bit Systems (3188128) (Critical)
Windows 10 Version 1607 for x64-based Systems	Not applicable	Windows 10 Version 1607 for x64-based Systems (3185614) (Important)	Windows 10 Version 1607 for x64-based Systems (3189866) (Important)	Windows 10 Version 1607 for x64-based Systems (3189866) (Critical)	Windows 10 Version 1607 for x64-based Systems (3188128) (Critical)
Windows 10 Version 1703 for 32-bit Systems	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable

Windows 10 Version 1703 for x64-based Systems	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
Server Core installation option					
Bulletin Identifier	**MS16-113**	**MS16-114**	**MS16-115**	**MS16-116**	**MS16-117**
Aggregate Severity Rating	**None**	**Important**	**None**	**Moderate**	**None**
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	Not applicable	Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (3177186) (Important)	Not applicable	Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (3184122) (Moderate)	Not applicable
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) (3177186) (Important)	Not applicable	Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) (3184122) (Moderate)	Not applicable
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3177186) (Important)	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3184122) (Moderate)	Not applicable
Windows Server 2012 (Server Core installation)	Not applicable	Windows Server 2012 (Server Core installation) (3177186) (Important)	Not applicable	Windows Server 2012 (Server Core installation) (3184122) (Moderate)	Not applicable
Windows Server 2012 R2 (Server Core installation)	Not applicable	Windows Server 2012 R2 (Server Core installation) (3177186) (Important)	Not applicable	Windows Server 2012 R2 (Server Core installation) (3184122) (Moderate)	Not applicable

Microsoft Office Suites and Software

Microsoft Office 2007	
Bulletin Identifier	**MS16-107**
Aggregate Severity Rating	**Critical**
Microsoft Office 2007 Service Pack 3	Microsoft Office 2007 Service Pack 3 (3118300) (Critical) Microsoft Excel 2007 Service Pack 3 (3115459) (Important) Microsoft Outlook 2007 (3118303)

	(Important) Microsoft PowerPoint 2007 Service Pack 3 (3114744) (Important)
Microsoft Office 2010	
Bulletin Identifier	**MS16-107**
Aggregate Severity Rating	**Critical**
Microsoft Office 2010 Service Pack 2 (32-bit editions)	Microsoft Office 2010 Service Pack 2 (32-bit editions) (3118309) (Critical) Microsoft Office 2010 Service Pack 2 (32-bit editions) (2553432) (Critical) Microsoft Excel 2010 Service Pack 2 (32-bit editions) (3118316) (Important) Microsoft Outlook 2010 Service Pack 2 (32-bit editions) (3118313) (Important) Microsoft PowerPoint 2010 Service Pack 2 (32-bit editions) (3115467) (Important)
Microsoft Office 2010 Service Pack 2 (64-bit editions)	Microsoft Office 2010 Service Pack 2 (64-bit editions) (3118309) (Critical) Microsoft Office 2010 Service Pack 2 (64-bit editions) (2553432) (Critical) Microsoft Excel 2010 Service Pack 2 (64-bit editions) (3118316) (Important) Microsoft Outlook 2010 Service Pack 2 (64-bit editions) (3118313) (Important) Microsoft PowerPoint 2010 Service Pack 2 (64-bit editions) (3115467) (Important)
Microsoft Office 2013	
Bulletin Identifier	**MS16-107**
Aggregate Severity Rating	**Critical**
Microsoft Office 2013 Service Pack 1 (32-bit editions)	Microsoft Office 2013 Service Pack 1 (32-bit editions) (3118268) (Critical) Microsoft Office 2013 Service Pack 1 (32-bit editions)[1] (Important)

	Microsoft Excel 2013 Service Pack 1 (32-bit editions) (3118284) (Important) Microsoft Outlook 2013 Service Pack 1 (32-bit editions) (3118280) (Important) Microsoft PowerPoint 2013 Service Pack 1 (32-bit editions) (3115487) (Important)
Microsoft Office 2013 Service Pack 1 (64-bit editions)	Microsoft Office 2013 Service Pack 1 (64-bit editions) (3118268) (Critical) Microsoft Office 2013 Service Pack 1 (64-bit editions)[1] (Important) Microsoft Excel 2013 Service Pack 1 (64-bit editions) (3118284) (Important) Microsoft Outlook 2013 Service Pack 1 (64-bit editions) (3118280) (Important) Microsoft PowerPoint 2013 Service Pack 1 (64-bit editions) (3115487) (Important)
Microsoft Office 2013 RT	
Bulletin Identifier	**MS16-107**
Aggregate Severity Rating	**Critical**
Microsoft Office 2013 RT Service Pack 1	Microsoft Office 2013 RT Service Pack 1 (3118268) (Critical) Microsoft Excel 2013 RT Service Pack 1 (3118284) (Important) Microsoft Outlook 2013 RT Service Pack 1 (3118280) (Important) Microsoft PowerPoint 2013 RT Service Pack 1 (3115487) (Important)
Microsoft Office 2016	
Bulletin Identifier	**MS16-107**
Aggregate Severity Rating	**Critical**
Microsoft Office 2016 (32-bit edition)	Microsoft Office 2016 (32-bit edition)[1] Microsoft Office 2016 (32-bit edition) (3118292) (Critical)

	Microsoft Excel 2016 (32-bit edition) (3118290) (Important) Microsoft Outlook 2016 (32-bit edition) (3118293) (Important) Microsoft Visio 2016 (32-bit editions) (Important)[1]
Microsoft Office 2016 (64-bit edition)	Microsoft Office 2016 (64-bit edition)[1] Microsoft Office 2016 (64-bit edition) (3118292) (Critical) Microsoft Excel 2016 (64-bit edition) (3118290) (Important) Microsoft Outlook 2016 (64-bit edition) (3118293) (Important) Microsoft Visio 2016 (64-bit editions) (Important)[1]
Microsoft Office for Mac 2011	
Bulletin Identifier	**MS16-107**
Aggregate Severity Rating	**Critical**
Microsoft Office for Mac 2011	Microsoft Word for Mac 2011 (3186805) (Critical)
Microsoft Office 2016 for Mac	
Bulletin Identifier	**MS16-107**
Aggregate Severity Rating	**Critical**
Microsoft Office 2016 for Mac	Microsoft Excel 2016 for Mac (3186807) (Important) Microsoft PowerPoint 2016 for Mac (3186807) (Important) Microsoft Word 2016 for Mac (3186807) (Critical) Microsoft Outlook 2016 for Mac (3186807) (Important)
Other Office Software	
Bulletin Identifier	**MS16-107**

Aggregate Severity Rating	**Critical**
Microsoft Office Compatibility Pack Service Pack 3	Microsoft Office Compatibility Pack Service Pack 3 (2597974) (Important) Microsoft Office Compatibility Pack Service Pack 3 (3115462) (Important)
Microsoft Excel Viewer	Microsoft Excel Viewer (3115463) (Important)
Microsoft PowerPoint Viewer	Microsoft PowerPoint Viewer (3054969) (Important)
Microsoft Word Viewer	Microsoft Word Viewer (3118297) (Critical)

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

Microsoft Office Services and Web Apps

Microsoft SharePoint Server 2007	
Bulletin Identifier	**MS16-107**
Aggregate Severity Rating	**Important**
Microsoft SharePoint Server 2007 Service Pack 3	Excel Services (3115112) (Important)
Microsoft SharePoint Server 2007 Service Pack 3 (64-bit editions)	Excel Services (3115112) (Important)
Microsoft SharePoint Server 2010	
Bulletin Identifier	**MS16-107**
Aggregate Severity Rating	**Critical**
Microsoft SharePoint Server 2010 Service Pack 2	Excel Services (3115119) (Important) Word Automation Services (3115466) (Critical)
Microsoft SharePoint Server 2013	
Bulletin Identifier	**MS16-107**
Aggregate Severity Rating	**Critical**

Microsoft SharePoint Server 2013 Service Pack 1	Microsoft SharePoint Server 2013 Service Pack 1 (3054862) (Critical) Excel Automation Services (3115169) (Critical) Word Automation Services (3115443) (Critical)
Microsoft Office Web Apps 2010	
Bulletin Identifier	**MS16-107**
Aggregate Severity Rating	**Critical**
Microsoft Office Web Apps 2010 Service Pack 2	Microsoft Office Web Apps 2010 Service Pack 2 (3115472) (Critical)
Microsoft Office Web Apps 2013	
Bulletin Identifier	**MS16-107**
Aggregate Severity Rating	**Critical**
Microsoft Office Web Apps Server 2013 Service Pack 1	Microsoft Office Web Apps Server 2013 Service Pack 1 (3118270) (Critical)
Microsoft Office Web Apps 2013	
Bulletin Identifier	**MS16-107**
Aggregate Severity Rating	**Important**
Office Online Server	Office Online Server (3118299) (Important)

Microsoft Server Software

Microsoft Exchange Server 2007	
Bulletin Identifier	**MS16-108**
Aggregate Severity Rating	**Important**
Microsoft Exchange Server 2007 Service Pack 3	Microsoft Exchange Server 2007 Service Pack 3 (3184711) (Important)
Microsoft Exchange Server 2010	
Bulletin Identifier	**MS16-108**
Aggregate Severity Rating	**Important**

Microsoft Exchange Server 2010 Service Pack 3	Microsoft Exchange Server 2010 Service Pack 3 (3184728) (Important)
Microsoft Exchange Server 2013	
Bulletin Identifier	**MS16-108**
Aggregate Severity Rating	**Important**
Microsoft Exchange Server 2013 Service Pack 1	Microsoft Exchange Server 2013 Service Pack 1 (3184736) (Important)
Microsoft Exchange Server 2013 Cumulative Update 12	Microsoft Exchange Server 2013 Cumulative Update 12 (3184736) (Important)
Microsoft Exchange Server 2013 Cumulative Update 13	Microsoft Exchange Server 2013 Cumulative Update 13 (3184736) (Important)
Microsoft Exchange Server 2016	
Bulletin Identifier	**MS16-108**
Aggregate Severity Rating	**Important**
Microsoft Exchange Server 2016 Cumulative Update 1	Microsoft Exchange Server 2016 Cumulative Update 1 (3184736) (Important)
Microsoft Exchange Server 2016 Cumulative Update 2	Microsoft Exchange Server 2016 Cumulative Update 2 (3184736) (Important)

Microsoft Developer Tools and Software

Microsoft Silverlight	
Bulletin Identifier	**MS16-109**
Aggregate Severity Rating	**Important**
Microsoft Silverlight 5	Microsoft Silverlight 5 when installed on Mac (3182373) (Important) Microsoft Silverlight 5 Developer Runtime when installed on Mac (3182373) (Important) Microsoft Silverlight 5 when installed on all supported releases of Microsoft Windows clients (3182373) (Important) Microsoft Silverlight 5 Developer Runtime when installed on all supported releases of Microsoft Windows clients (3182373) (Important)

	Microsoft Silverlight 5 when installed on all supported releases of Microsoft Windows servers (3182373) (Important)

Detection and Deployment Tools and Guidance

Several resources are available to help administrators deploy security updates.

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

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

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

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

Acknowledgments

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

Other Information

Microsoft Windows Malicious Software Removal Tool

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

Non-Security Updates on MU, WU, and WSUS

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

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

Microsoft Active Protections Program (MAPP)

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

Security Strategies and Community

Update Management Strategies

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

Obtaining Other Security Updates

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

- Security updates are available from Microsoft Download Center. You can find them most easily by doing a keyword search for "security update".
- Updates for consumer platforms are available from Microsoft Update.
- You can obtain the security updates offered this month on Windows Update, from Download Center on Security and Critical Releases ISO CD Image files. For more information, see Microsoft Knowledge Base Article 913086.

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 (September 13, 2016): Bulletin Summary published.
- V2.0 (July 11, 2017): For MS16-111, added Windows 10 Version 1703 for 32-bit Systems and Windows 10 Version 1703 for x64-based Systems to the Affected Software table because they are affected by CVE-2016-3305. Microsoft recommends that customers running Windows 10 Version 1703 should install update 4025342 to be protected from this vulnerability.

Page generated 2017-07-11 08:15-07:00.