Microsoft Security Bulletin Summary for January 2017

Published: January 10, 2017 | Updated: January 10, 2017

Version: 1.1

This bulletin summary lists security bulletins released for January 2017.

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

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

Note: There are no security fixes or quality improvements for Windows 8.1, Windows Server 2012, or Windows Server 2012 R2 for release on Update Tuesday for January 2017. As such, there is no Security Only Quality Update or Security Monthly Quality Rollup release for these platforms this month.

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

On this page

Executive Summaries

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

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

Bulletin ID	Bulletin Title and Executive Summary	Maximum Severity Rating and Vulnerability Impact	Restart Requirement	Known Issues	Affected Software
MS17-001	**Security Update for Microsoft Edge (3214288)** This security update resolves a vulnerability in Microsoft Edge. This vulnerability could allow an elevation of privilege if a user views a specially crafted webpage using Microsoft Edge. An attacker who successfully exploited this vulnerability could gain elevated permissions on the namespace directory of a vulnerable system and gain elevated privileges	Important Elevation of Privilege	Requires restart	----------	Microsoft Windows, Microsoft Edge
MS17-002	**Security Update for Microsoft Office (3214291)** This security update resolves a vulnerability in Microsoft Office. The vulnerability could allow remote code execution if a user opens a specially crafted Microsoft Office file. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. Customers whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.	Important Remote Code Execution	May require restart	----------	Microsoft Office, Microsoft Office Services and Web Apps

MS17-003	**Security Update for Adobe Flash Player (3214628)** This security update resolves vulnerabilities in Adobe Flash Player when installed on all supported editions of Windows 8.1, Windows Server 2012, Windows Server 2012 R2, Windows RT 8.1, Windows 10, and Windows Server 2016.	Critical Remote Code Execution	Requires restart	---------	Microsoft Windows, Adobe Flash Player
MS17-004	**Security Update for Local Security Authority Subsystem Service (3216771)** A denial of service vulnerability exists in the way the Local Security Authority Subsystem Service (LSASS) handles authentication requests. An attacker who successfully exploited the vulnerability could cause a denial of service on the target system's LSASS service, which triggers an automatic reboot of the system. The security update addresses the vulnerability by changing the way that LSASS handles specially crafted authentication requests.	Important Denial of Service	Requires restart	---------	Microsoft Windows

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
MS17-001: Security Update for Microsoft Edge (3214288)				
CVE-2017-0002	Microsoft Edge Elevation of Privilege Vulnerability	1- Exploitation More Likely	4 - Not affected	Not applicable
MS17-002: Security Update for Microsoft Office (3214291)				
CVE-2017-0003	Microsoft Office Memory Corruption Vulnerability	1- Exploitation More Likely	4 - Not affected	Not applicable
MS17-003 Security Update for Adobe Flash Player (3214628)				
APSB17-02	See Adobe Security Bulletin APSB17-02 for vulnerability severity and	---------	---------	Not applicable

	update priority ratings.			
MS17-004 Security Update for Local Security Authority Subsystem Service (3216771)				
CVE-2017-0004	Local Security Authority Subsystem Service Denial of Service Vulnerability	4 - Not affected	3 - Exploitation Unlikely	Permanent

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

Windows Vista			
Bulletin Identifier	**MS17-001**	**MS17-003**	**MS17-004**
Aggregate Severity Rating	**None**	**None**	**Important**
Windows Vista for Service Pack 2	Not applicable	Not applicable	Windows Vista for Service Pack 2 (3216775) (Important)
Windows Vista x64 Edition Service Pack 2	Not applicable	Not applicable	Windows Vista x64 Edition Service Pack 2 (3216775) (Important)
Windows Server 2008			
Bulletin Identifier	**MS17-001**	**MS17-003**	**MS17-004**
Aggregate Severity Rating	**None**	**None**	**Important**
Windows Server 2008 for 32-bit Systems Service Pack 2	Not applicable	Not applicable	Windows Server 2008 for 32-bit Systems Service Pack 2 (3216775) (Important)
Windows Server 2008 for x64-based Systems Service Pack 2	Not applicable	Not applicable	Windows Server 2008 for x64-based Systems Service Pack 2 (3216775) (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 (3216775) (Important)
Windows 7			

Bulletin Identifier	MS17-001	MS17-003	MS17-004
Aggregate Severity Rating	**None**	**None**	**Important**
Windows 7 for x32-bit Systems Service Pack 1 Security Only	Not applicable	Not applicable	Windows 7 for x32-bit Systems Service Pack 1 (3212642) (Important)
Windows 7 for x64-based Systems Service Pack 1 Monthly Rollup	Not applicable	Not applicable	Windows 7 for x64-based Systems Service Pack 1 (3212646) (Important)
Windows 7 for x32-bit Systems Service Pack 1 Security Only	Not applicable	Not applicable	Windows 7 for x32-bit Systems Service Pack 1 (3212642) (Important)
Windows 7 for x64-based Systems Service Pack 1 Monthly Rollup	Not applicable	Not applicable	Windows 7 for x64-based Systems Service Pack 1 (3212646) (Important)
Windows Server 2008 R2			
Bulletin Identifier	**MS17-001**	**MS17-003**	**MS17-004**
Aggregate Severity Rating	**None**	**None**	**Important**
Windows Server 2008 R2 for x64-based Systems Service Pack 1 Security Only	Not applicable	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack (3212642) (Important)
Windows Server 2008 R2 for x64-based Systems Service Pack 1 Monthly Rollup	Not applicable	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3212646) (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 (3212642) (Important)
Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 Monthly Rollup	Not applicable	Not applicable	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3212646) (Important)
Windows 8.1			
Bulletin Identifier	**MS17-001**	**MS17-003**	**MS17-004**
Aggregate Severity Rating	**None**	**Critcal**	**None**
Windows 8.1 for 32-bit Systems Security Only	Not applicable	Adobe Flash Player (3214628) (Critical)	Not applicable
Windows 8.1 for 32-bit Systems Monthly Rollup	Not applicable	Not applicable	Not applicable
Windows 8.1 for x64-based Systems Security Only	Not applicable	Adobe Flash Player	Not applicable

		(3214628) (Critical)	
Windows 8.1 for x64-based Systems Monthly Rollup	Not applicable	Not applicable	Not applicable
Windows Server 2012 and Windows Server 2012 R2			
Bulletin Identifier	**MS17-001**	**MS17-003**	**MS17-004**
Aggregate Severity Rating	**None**	**Moderate**	**None**
Windows Server 2012 Security Only	Not applicable	Adobe Flash Player (3214628) (Moderate)	Not applicable
Windows Server 2012 Monthly Rollup	Not applicable	Not applicable	Not applicable
Windows Server 2012 R2 Security Only	Not applicable	Adobe Flash Player (3214628) (Moderate)	Not applicable
Windows Server 2012 R2 Monthly Rollup	Not applicable	Not applicable	Not applicable
Windows RT 8.1			
Bulletin Identifier	**MS17-001**	**MS17-003**	**MS17-004**
Aggregate Severity Rating	**None**	**Critical**	**None**
Windows RT 8.1 Monthly Rollup	Not applicable	Adobe Flash Player (3214628) (Critical)	Not applicable
Windows 10			
Bulletin Identifier	**MS17-001**	**MS17-003**	**MS17-004**
Aggregate Severity Rating	**Important**	**Critical**	**None**
Windows 10 for 32-bit Systems	Microsoft Edge (3210720) (Critical)	Adobe Flash Player (3214628) (Critical)	Not applicable
Windows 10 for x64-based Systems	Microsoft Edge (3210720) (Critical)	Adobe Flash Player (3214628) (Critical)	Not applicable
Windows 10 Version 1511 for 32-bit Systems	Microsoft Edge (3210721) (Critical)	Adobe Flash Player (3214628) (Critical)	Not applicable
Windows 10 Version 1511 for x64-based Systems	Microsoft Edge (3210721) (Critical)	Adobe Flash Player (3214628) (Critical)	Not applicable

Windows 10 Version 1607 for 32-bit Systems	Microsoft Edge (3211320) (Critical)	Adobe Flash Player (3214628) (Critical)	Not applicable
Windows 10 Version 1607 for x64-based Systems	Microsoft Edge (3211320) (Critical)	Adobe Flash Player (3214628) (Critical)	Not applicable
Windows Server 2016			
Bulletin Identifier	**MS17-001**	**MS17-003**	**MS17-004**
Aggregate Severity Rating	**Moderate**	**Critical**	**None**
Windows Server 2016 for x64-based Systems	Microsoft Edge (3211320) (Moderate)	Adobe Flash Player (3214628) (Critical)	Not applicable
Server Core installation option			
Bulletin Identifier	**MS17-001**	**MS17-003**	**MS17-004**
Aggregate Severity Rating	**Moderate**	**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) (3216775) (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) (3216775) (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 (Server Core installation) (3212642) (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) (3212646) (Important)
Windows Server 2012 (Server Core installation) Security Only	Not applicable	Not applicable	Not applicable
Windows Server 2012 (Server Core installation) Monthly Rollup	Not applicable	Not applicable	Not applicable
Windows Server 2012 R2 (Server Core installation) Security Only	Not applicable	Not applicable	Not applicable
Windows Server 2012 R2 (Server Core installation) Monthly Rollup	Not applicable	Not applicable	Not applicable

Windows Server 2016 for x64-based Systems (Server Core installation)	Not applicable	Not applicable	Not applicable

Microsoft Office Suites and Software

Microsoft Office 2016	
Bulletin Identifier	**MS17-002**
Aggregate Severity Rating	**Important**
Microsoft Office 2016 (32-bit edition)	Microsoft Word 2016 (32-bit edition) (3128057) (Important)
Microsoft Office 2016 (64-bit edition)	Microsoft Word 2016 (64-bit edition) (3128057) (Important)

Microsoft Office Services and Web Apps

Microsoft Office Services and Web Apps	**Microsoft Office Services and Web Apps**
Bulletin Identifier	**MS17-002**
Aggregate Severity Rating	**Important**
Microsoft SharePoint Enterprise Server 2016 64-Bit Edition	Microsoft SharePoint Foundation 2016 64-Bit Edition (3141486) (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 (January 10, 2017): Bulletin Summary published.
- V1.1 (January 10, 2017): Bulletin Summary revised to change the severity of CVE-2017-0003 to Important. This is an informational change only.

Page generated 2017-02-06 10:33-08:00.