

Microsoft Security Bulletin Summary for February 2017

Published: February 21, 2017

Version: 1.0

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

As a reminder, the [Security Updates Guide](#) will be replacing security bulletins. Please see our blog post, [Furthering our commitment to security updates](#), for more details.

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 next section, **Affected Software**.

Bulletin ID	Bulletin Title and Executive Summary	Maximum Severity Rating and Vulnerability Impact	Restart Requirement	Known Issues	Affected Software
MS17-005	Security Update for Adobe Flash Player (4010250) 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

Exploitability Index

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

How do I use this table?

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

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

CVE ID	Vulnerability Title	Exploitability Assessment for	Exploitability Assessment for	Denial of Service
--------	---------------------	-------------------------------	-------------------------------	-------------------

		Latest Software Release	Older Software Release	Exploitability Assessment
MS17-005: Security Update for Adobe Flash Player (4010250)				
APSB17-04	See Adobe Security Bulletin APSB17-04 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

Windows 8.1	
Bulletin Identifier	MS17-005
Aggregate Severity Rating	Critical
Windows 8.1 for 32-bit Systems Security Only	Adobe Flash Player (4010250) (Critical)
Windows 8.1 for 32-bit Systems Monthly Rollup	Not applicable
Windows 8.1 for x64-based Systems Security Only	Adobe Flash Player (4010250) (Critical)
Windows 8.1 for x64-based Systems Monthly Rollup	Not applicable
Windows Server 2012 and Windows Server 2012 R2	
Bulletin Identifier	MS17-005
Aggregate Severity Rating	Moderate
Windows Server 2012 Security Only	Adobe Flash Player (4010250) (Moderate)
Windows Server 2012 Monthly Rollup	Not applicable
Windows Server 2012 R2 Security Only	Adobe Flash Player (4010250) (Moderate)

Windows Server 2012 R2 Monthly Rollup	Not applicable
Windows RT 8.1	
Bulletin Identifier	MS17-005
Aggregate Severity Rating	Critical
Windows RT 8.1 Monthly Rollup	Adobe Flash Player (4010250) (Critical)
Windows 10	
Bulletin Identifier	MS17-005
Aggregate Severity Rating	Critical
Windows 10 for 32-bit Systems	Adobe Flash Player (4010250) (Critical)
Windows 10 for x64-based Systems	Adobe Flash Player (4010250) (Critical)
Windows 10 Version 1511 for 32-bit Systems	Adobe Flash Player (4010250) (Critical)
Windows 10 Version 1511 for x64-based Systems	Adobe Flash Player (4010250) (Critical)
Windows 10 Version 1607 for 32-bit Systems	Adobe Flash Player (4010250) (Critical)
Windows 10 Version 1607 for x64-based Systems	Adobe Flash Player (4010250) (Critical)
Windows Server 2016	
Bulletin Identifier	MS17-005
Aggregate Severity Rating	Critical
Windows Server 2016 for x64-based Systems	Adobe Flash Player (4010250) (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](#).
- 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

The information provided in the Microsoft Knowledge Base is provided "as is" without warranty of any kind. Microsoft disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall Microsoft Corporation or its suppliers be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Microsoft Corporation or its suppliers have been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages so the foregoing limitation may not apply.

Revisions

- V1.0 (February 21, 2017): Bulletin Summary published.

Page generated 2017-02-21 07:05-08:00.

© 2017 Microsoft