Microsoft Security Advisory 3033929

Availability of SHA-2 Code Signing Support for Windows 7 and Windows Server 2008 R2

Published: March 10, 2015

Version: 1.0

General Information

On this page

Executive Summary

Microsoft is announcing the reissuance of an update for all supported editions of Windows 7 and Windows Server 2008 R2 to add support for SHA-2 signing and verification functionality. This update supersedes the 2949927 update that was rescinded on October 17, 2014 to address issues that some customers experienced after installation. As with the original release, Windows 8, Windows 8.1, Windows Server 2012, Windows Server 2012 R2, Windows RT, and Windows RT 8.1 do not require this update because SHA-2 signing and verification functionality is already included in these operating systems. This update is not available for Windows Server 2003, Windows Vista, or Windows Server 2008.

Recommendation. Customers who have automatic updating enabled and configured to check online for updates from Microsoft Update typically will not need to take any action because this security update will be downloaded and installed automatically. Customers who have not enabled automatic updating need to check for updates and install this update manually. For information about specific configuration options in automatic updating, see Microsoft Knowledge Base Article 294871.

For customers who install updates manually (including customers who have not enabled automatic updating), Microsoft recommends applying the update at the earliest opportunity using update management software, or by checking for updates using the Microsoft Update service. The updates are also available via the download links in the **Affected Software** table in this advisory.

Advisory Details

Issue References

For more information about this issue, see the following references:

References	Identification
Microsoft Knowledge Base Article	3033929 (supersedes 2949927)

Affected Software

This advisory discusses the following software.

Operating System	Updates Replaced
Windows 7 for 32-bit Systems Service Pack 1 (3033929)[1]	3035131 in MS15-025
Windows 7 for x64-based Systems Service Pack 1 (3033929)[1]	3035131 in MS15-025
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3033929)[1]	3035131 in MS15-025
Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3033929)[1]	3035131 in MS15-025
Server Core installation option	3035131 in MS15-025
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3033929)[1]	3035131 in MS15-025

[1]The 3033929 update has affected binaries in common with the 3035131 update being released simultaneously via MS15-025. Customers who download and install updates manually and who are planning to install both updates should install the 3035131 update before installing the 3033929 update. See the Advisory FAQ for more information.

Advisory FAQ

What is the scope of the advisory?
The purpose of this advisory is to inform customers of an update that adds functionality for the SHA-2 hashing algorithm to all supported editions of Windows 7 and Windows Server 2008 R2.

Is this a security vulnerability that requires Microsoft to issue a security update?
No. A signing mechanism alternative to SHA-1 has been available for some time, and the use of SHA-1 as a hashing algorithm for signing purposes has been discouraged and is no longer a best practice. Microsoft recommends using the SHA-2 hashing algorithm instead and is releasing this update to enable customers to migrate digital certificate keys to the more secure SHA-2 hashing algorithm.

What is the cause of the problem with the SHA-1 hashing algorithm?
The root cause of the problem is a known weakness of the SHA-1 hashing algorithm that exposes it to collision attacks. Such attacks could allow an attacker to generate additional certificates that have the same digital signature as an original. These issues are well understood and the use of SHA-1 certificates for specific purposes that require resistance against these attacks has been discouraged. At Microsoft, the Security Development Lifecycle has required Microsoft to no longer use the SHA-1 hashing algorithm as a default functionality in Microsoft software. For more information, see Microsoft Security Advisory 2880823 and the Windows PKI blog entry, SHA1 Deprecation Policy.

What does the update do?
The update adds SHA-2 hashing algorithm signing and verification support to affected operating systems, which includes the following:

- Support for multiple signatures on Cabinet files
- Support for multiple signatures for Windows PE files
- UI changes that enable the viewing multiple digital signatures
- The ability to verify RFC3161 timestamps to the Code Integrity component that verifies signatures in the kernel
- Support for various APIs, including CertIsStrongHashToSign, CryptCATAdminAcquireContext2 and CryptCATAdminCalcHashFromFileHandle2

What is Secure Hash Algorithm (SHA-1)?
The Secure Hash Algorithm (SHA) was developed for use with the Digital Signature Algorithm (DSA) or the Digital Signature Standard (DSS) and generates a 160-bit hash value. SHA-1 has known weaknesses that exposes it to collision attacks. Such attacks could allow an attacker to generate additional certificates that have the same digital signature as an original. For more information about SHA-1, see Hash and Signature Algorithms.

What is RFC3161?
RFC3161 defines the Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) describing the format of requests and responses to a Time Stamping Authority (TSA). The TSA is can be used to prove that a digital signature was generated during the validity period of a public key certificate, see X.509 Public Key Infrastructure.

What is a digital certificate?
In public key cryptography, one of the keys, known as the private key, must be kept secret. The other key, known as the public key, is intended to be shared with the world. However, there must be a way for the owner of the key to tell the world to whom the key belongs. Digital certificates provide a way to do this. A digital certificate is an electronic credential used to certify the online identities of individuals, organizations, and computers. Digital certificates contain a public key packaged together with information about it (who owns it, what it can be used for, when it expires, and so forth). For more information, see Understanding Public Key Cryptography and Digital Certificates.

What is the purpose of a digital certificate?
Digital certificates are used primarily to verify the identity of a person or device, authenticate a service, or encrypt files. Normally, there is no need to think about certificates at all, aside from the occasional message stating that a certificate is expired or invalid. In such cases, one should follow the instructions provided in the message.

How is this update (3033929) related to the 3035131 update discussed in MS15-025?
This update (3033929) shares affected binaries with the 3035131 update being released simultaneously via MS15-025. This overlap necessitates that one update supersede the other and, in this case, advisory update 3033929 supersedes update 3035131. Customers with automatic updating enabled should experience no unusual installation behavior; both updates should install automatically and both should appear in the list of installed updates. However, for customers who download and install updates manually, the order in which the updates are installed will determine the observed behavior as follows:

Scenario 1 (preferred): Customer first installs update 3035131 and then installs advisory update 3033929.
Result: Both updates should install normally and both updates should appear in the list of installed updates.

Scenario 2: Customer first installs advisory update 3033929 and then attempts to install update 3035131.
Result: The installer notifies the user that the 3035131 update is already installed on the system; and the 3035131 update is NOT added to the list of installed updates.

Suggested Actions

- **Apply the update for supported releases of Microsoft Windows**
  The majority of customers have automatic updating enabled and will not need to take any action because the update will be downloaded and installed automatically. Customers who have not enabled automatic updating need to check for updates and install this update manually. For information about specific configuration options in automatic updating, see Microsoft Knowledge Base Article 294871.

  For administrators and enterprise installations, or end users who want to install this security update manually (including customers who have not enabled automatic updating), Microsoft recommends that customers apply the update at the earliest opportunity using update management software, or by checking for updates using the Microsoft Update service. The updates are also available via the download links in the **Affected Software** table in this advisory.

Additional Suggested Actions

- **Protect your PC**
  We continue to encourage customers to follow our Protect Your Computer guidance of enabling a firewall, getting software updates and installing antivirus software. For more information, see Microsoft Safety & Security Center.

- **Keep Microsoft Software Updated**
  Users running Microsoft software should apply the latest Microsoft security updates to help make sure that their computers are as protected as possible. If you are not sure whether your software is up to date, visit Microsoft Update, scan your computer for available updates, and install any high-priority updates that are offered to you. If you have automatic updating enabled and configured to provide updates for Microsoft products, the updates are delivered to you when they are released, but you should verify that they are installed.

Other Information

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.

Feedback

- You can provide feedback by completing the Microsoft Help and Support form, Customer Service Contact Us.

Support

- Customers in the United States and Canada can receive technical support from Security Support. For more information, see Microsoft Help and Support.
- International customers can receive support from their local Microsoft subsidiaries. For more information, see International Support.
- Microsoft TechNet Security provides additional information about security in Microsoft products.

Disclaimer

Revisions

- V1.0 (March 10, 2015): Advisory published.

Page generated 2015-03-04 14:52Z-08:00.