Learn   Discover ⌄   Product documentation ⌄   Development languages ⌄   Topics ⌄   🔍   Sign in

⊕   ⋮

Microsoft Security Advisory 4022344

Article • 10/14/2022 • 4 contributors   👍 Feedback

In this article

Security Update for Microsoft Malware Protection Engine

Executive Summary

Advisory Details

Affected Software

Show 6 more

Security Update for Microsoft Malware Protection Engine

Published: May 8, 2017 | Updated: May 12, 2017

Version: 1.2

Executive Summary

Microsoft is releasing this security advisory to inform customers that an update to the Microsoft Malware Protection Engine addresses a security vulnerability that was reported to Microsoft.

The update addresses a vulnerability that could allow remote code execution if the Microsoft Malware Protection Engine scans a specially crafted file. An attacker who successfully exploited this vulnerability could execute arbitrary code in the security context of the LocalSystem account and take control of the system.

The Microsoft Malware Protection Engine ships with several Microsoft antimalware products. See the **Affected Software** section for a list of affected products. Updates to the Microsoft Malware Protection Engine are installed along with the updated malware definitions for the affected products. Administrators of enterprise installations should follow their established internal processes to ensure that the definition and engine updates are approved in their update management software, and that clients consume the updates accordingly.

Typically, no action is required of enterprise administrators or end users to install updates for the Microsoft Malware Protection Engine, because the built-in mechanism for the automatic detection and deployment of updates will apply the update within 48 hours of release. The exact time frame depends on the software used, Internet connection, and infrastructure configuration.

The information in this advisory is also available in the Security Update Guide referenced by CVE-2017-0290 ⬀ .

Advisory Details

Issue References

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

⌞⌝ **Expand table**

References	Identification
Last version of the Microsoft Malware Protection Engine affected by this vulnerability	Version 1.1.13701.0
First version of the Microsoft Malware Protection Engine with this vulnerability addressed	Version 1.1.13704.0

* If your version of the Microsoft Malware Protection Engine is equal to or greater than this version, then you are not affected by this vulnerability and do not need to take any further action. For more information on how to verify the engine version number that your software is currently using, see the section, "Verifying Update Installation", in Microsoft Knowledge Base Article 2510781 ⧉ .

Affected Software

The following software versions or editions are affected. Versions or editions that are not listed are either past their support life cycle or are not affected. To determine the support life cycle for your software version or edition, see Microsoft Support Lifecycle ⧉ .

⌞⌝ **Expand table**

Antimalware Software	Microsoft Malware Protection Engine Remote Code Execution Vulnerability ⧉ - **CVE-2017-0290**
Microsoft Forefront Endpoint Protection 2010	**Critical** \ Remote Code Execution
Microsoft Endpoint Protection	**Critical** \ Remote Code Execution
Microsoft System Center Endpoint Protection	**Critical** \ Remote Code Execution

Microsoft Security Essentials	**Critical** \ Remote Code Execution
Windows Defender for Windows 7	**Critical** \ Remote Code Execution
Windows Defender for Windows 8.1	**Critical** \ Remote Code Execution
Windows Defender for Windows RT 8.1	**Critical** \ Remote Code Execution
Windows Defender for Windows 10, Windows 10 1511, Windows 10 1607, Windows Server 2016, Windows 10 1703	**Critical** \ Remote Code Execution
Windows Intune Endpoint Protection	**Critical** \ Remote Code Execution
Microsoft Exchange Server 2013	**Critical** \ Remote Code Execution
Microsoft Exchange Server 2016	**Critical** \ Remote Code Execution
Microsoft Windows Server 2008 R2	**Critical** \ Remote Code Execution

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.

⌞⌝ **Expand table**

CVE ID	Vulnerability Title	Exploitability Assessment for\ Latest Software Release	Exp Ol
CVE-2017-0290 ⧉	Scripting Engine Memory Corruption Vulnerability	2 - Exploitation Less Likely	2 -

Advisory FAQ

Is Microsoft releasing a Security Bulletin to address this vulnerability?
No. Microsoft is releasing this informational security advisory to inform customers that an update to the Microsoft Malware Protection Engine addresses a security vulnerability that was reported to Microsoft.

Typically, no action is required of enterprise administrators or end users to install this update.

Why is no action required to install this update?
In response to a constantly changing threat landscape, Microsoft frequently updates malware definitions and the Microsoft Malware Protection Engine. In order to be effective in helping protect against new and prevalent threats, antimalware software must be kept up to date with these updates in a timely manner.

For enterprise deployments as well as end users, the default configuration in Microsoft antimalware software helps ensure that malware definitions and the Microsoft Malware Protection Engine are kept up to date automatically. Product documentation also recommends that products are configured for automatic updating.

Best practices recommend that customers regularly verify whether software distribution, such as the automatic deployment of Microsoft Malware Protection Engine updates and malware definitions, is working as expected in their environment.

How often are the Microsoft Malware Protection Engine and malware definitions updated?
Microsoft typically releases an update for the Microsoft Malware Protection Engine once a month or as needed to protect against new threats. Microsoft also typically updates the malware definitions three times daily and can increase the frequency when needed.

Depending on which Microsoft antimalware software is used and how it is configured, the software may search for engine and definition updates every day when connected to the Internet, up to multiple times daily. Customers can also choose to manually check for updates at any time.

How can I install the update?
Refer to the section, **Suggested Actions**, for details on how to install this update.

What is the Microsoft Malware Protection Engine?
The Microsoft Malware Protection Engine, mpengine.dll, provides the scanning, detection, and cleaning capabilities for Microsoft antivirus and antispyware software.

Does this update contain any additional security-related changes to functionality?
Yes. In addition to the changes that are listed for this vulnerability, this update includes defense-in-depth updates to help improve security-related features.

Where can I find more information about Microsoft antimalware technology?
For more information, visit the Microsoft Malware Protection Center website.

Microsoft Malware Protection Engine Remote Code Execution Vulnerability - CVE-2017-0290

A remote code execution vulnerability exists when the Microsoft Malware Protection Engine does not properly scan a specially crafted file leading to memory corruption.

An attacker who successfully exploited this vulnerability could execute arbitrary code in the security context of the LocalSystem account and take control of the system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

To exploit this vulnerability, a specially crafted file must be scanned by an affected version of the Microsoft Malware Protection Engine. There are many ways that an attacker could place a specially crafted file in a location that is scanned by the Microsoft Malware Protection Engine. For example, an attacker could use a website to deliver a specially crafted file to the victim's system that is scanned when the website is viewed by the user. An attacker could also deliver a specially crafted file via an email message or in an Instant Messenger message that is scanned when the file is opened. In addition, an attacker could take advantage of websites that accept or host user-provided content, to upload a specially crafted file to a shared location that is scanned by the Malware Protection Engine running on the hosting server.

If the affected antimalware software has real-time protection turned on, the Microsoft Malware Protection Engine will scan files automatically, leading to exploitation of the vulnerability when the specially crafted file scanned. If real-time scanning is not enabled, the attacker would need to wait until a scheduled scan occurs in order for the vulnerability to be exploited. All systems running an affected version of antimalware software are primarily at risk.

The update addresses the vulnerability by correcting the manner in which the Microsoft Malware Protection Engine scans specially crafted files.

Microsoft received information about this vulnerability through coordinated vulnerability disclosure.

Microsoft had not received any information to indicate that this vulnerability had been publicly used to attack customers when this security advisory was originally issued.

Suggested Actions

- **Verify that the update is installed**
  Customers should verify that the latest version of the Microsoft Malware Protection Engine and definition updates are being actively downloaded and installed for their Microsoft antimalware products.

  For more information on how to verify the version number for the Microsoft Malware Protection Engine that your software is currently using, see the section, "Verifying Update Installation", in Microsoft Knowledge Base Article 2510781 ☒ .

  For affected software, verify that the Microsoft Malware Protection Engine version is 1.1.13704.0 or later.

- **If necessary, install the update**
  Administrators of enterprise antimalware deployments should ensure that their update management software is configured to automatically approve and distribute engine updates and new malware definitions. Enterprise administrators should also verify that the latest version of the Microsoft Malware Protection Engine and definition updates are being actively downloaded, approved and deployed in their environment.

For end-users, the affected software provides built-in mechanisms for the automatic detection and deployment of this update. For these customers, the update will be applied within 48 hours of its availability. The exact time frame depends on the software used, Internet connection, and infrastructure configuration. End users that do not wish to wait can manually update their antimalware software.

For more information on how to manually update the Microsoft Malware Protection Engine and malware definitions, refer to Microsoft Knowledge Base Article 2510781 ⧉ .

Acknowledgments

Microsoft thanks ⧉ the following for working with us to help protect customers:

- Natalie Silvanovich and Tavis Ormandy of Google Project Zero ⧉

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

The information provided in this advisory 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 (May 8, 2017): Advisory published.
- V1.1 (May 11, 2017): Added link to the same information in the Security Update Guide. This is an informational change only.

- V1.2 (May 12, 2017): Added entries into the affected software table. This is an informational change only.

Page generated 2017-06-14 10:20-07:00.

🌐 **English (United States)**   ✔✗ **Your Privacy Choices**   ☼ **Theme** ⌄

Manage cookies   Previous Versions   Blog ⧉   Contribute   Privacy ⧉   Terms of Use   Trademarks ⧉

© Microsoft 2024