CERT-EU Security Advisory 2017-011

Critical Microsoft Scripting Engine Memory Corruption Vulnerability

May 10, 2017 — v1.0

History:

- *10/05/2017 — v1.0: Initial publication*

Summary

On Saturday, 6th of May 2017, Tavis Ormandy and Natalie Silvanovich of Google Project Zero discovered a Remote Code Execution (RCE) vulnerability (CVE-2017-0290) [1] affecting Windows Defender and other products.

On Monday, 8th of May 2017, Microsoft has released a Security Advisory 4022344 [2] providing more details about the vulnerability and about products affected by it. On the same day, Microsoft issued an emergency out-of-band security update to patch the above vulnerability in Microsoft Malware Protection Engine. The update addresses a vulnerability that allows remote code execution if the Microsoft Malware Protection Engine scans a specially crafted file. An attacker who successfully exploits this vulnerability could execute arbitrary code in the security context of the LocalSystem account and take control of the system.

Technical Details

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 exploits 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.

Tavis Ormandy has reported on the Chromium bug forum [6] that `MsMpEng` – the Malware Protection service enabled by default on the majority of Windows versions – runs as `NT AUTHORITY\SYSTEM` without sandboxing and is remotely accessible without authentication via various Windows services, including Exchange, IIS and the provided proof-of-concept of the vulnerability [6]. `NScript` is the component of `mpengine.dll` that evaluates any filesystem or network activity that looks like JavaScript. `NScript` is a un-sandboxed and highly privileged JavaScript interpreter that is used to evaluate untrusted code, by default on the majority of all modern Windows systems.

The official Microsoft response is that the Microsoft Malware Protection Engine, `mpengine.dll`, provides the scanning, detection, and cleaning capabilities for Microsoft antivirus and antispyware software.

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 user views the website. An attacker could also deliver a specially crafted file via an email message (reading the email or opening attachments is not necessary) 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 anti-malware software has real-time protection turned on, the Microsoft Malware Protection Engine will scan files automatically, since `MsMpEng` uses a filesystem mini-filter to intercept and inspect all system filesystem activity leading to exploitation of the vulnerability when the specially crafted file is 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 anti-malware software are primarily at risk.

Products Affected

The following software versions or editions are affected:

- Microsoft Forefront Endpoint Protection 2010
- Microsoft Endpoint Protection
- Microsoft Forefront Security for SharePoint Service Pack 3
- Microsoft System Center Endpoint Protection
- Microsoft Security Essentials
- Windows Defender for Windows 7
- Windows Defender for Windows 8.1
- Windows Defender for Windows RT 8.1
- Windows Defender for Windows 10, Windows 10 1511, Windows 10 1607, Windows Server 2016, Windows 10 1703
- Windows Intune Endpoint Protection

In addition, other products not mentioned here that are past their support life could be affected.

Recommendations

Typically, no action is required of enterprise administrators or end-users to install updates for the Microsoft Malware Protection Engine. The affected software provides built-in mechanisms for the automatic detection and deployment of this update but its possible to update it also manually [4, 5]. The update will be applied within 48 hours of its availability. The exact period depends on the software used, Internet connection, and infrastructure configuration.

Administrators of enterprise anti-malware 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.

A verification [3] should be done that the latest version of the Microsoft Malware Protection Engine and definition updates are being actively downloaded and installed for their Microsoft anti-malware products and that Microsoft Malware Protection Engine version is `1.1.13704.0` or later.

References

[1] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0290

[2] https://technet.microsoft.com/en-us/library/security/4022344.aspx

[3] https://support.microsoft.com/kb/2510781

[4] https://support.microsoft.com/en-us/help/923159/how-to-manually-download-the-latest-definition-updates-for-windows-defender

[5] https://support.microsoft.com/en-us/help/2510781/microsoft-malware-protection-engine-deployment-information

[6] https://bugs.chromium.org/p/project-zero/issues/detail?id=1252&desc=5