Tugas Keamanan Jaringan Komputer

DISUSUN OLEH

NAMA : ANNISA SOLEHA

NIM : 09011181419038

SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2018

Microsoft Malware Protection Engine Remote Code Execution Vulnerability

CVE-ID : CVE-2017-8542

Description : The Microsoft Malware Protection Engine running on Microsoft Forefront and Microsoft Defender on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016, Microsoft Exchange Server 2013 and 2016, does not properly scan a specially crafted file leading to denial of service. aka "Microsoft Malware Protection Engine Denial of Service Vulnerability".

Banyaknya kerentanan terhadap microsoft malware protection engine telah dilaporkan. Seorang remote user dapat menyebabkan kode berubah-ubah saat dieksekusi pada sistem target. Sedangkan local user dapat menyebabkan penolakan terhadap kondisi pelayanan di sistem target. Seorang remote user membuat file yang dibuat khusus, dimanan saat file tersebut dipindai oleh target, microsoft malware protection engine akan mengeksekusi kode acak pada sistem target. Kode akan berjalan dengan local system privileges. Sehingga menyebabkan timeout scan pada sistem target, akibatnya layanan microsoft malware protection engine tidak akan memantau sistem sampai layanan di restart.

Mateusz Jurczyk dari Project Zero Google yang melaporkan hal ini.

Cause : Access control error

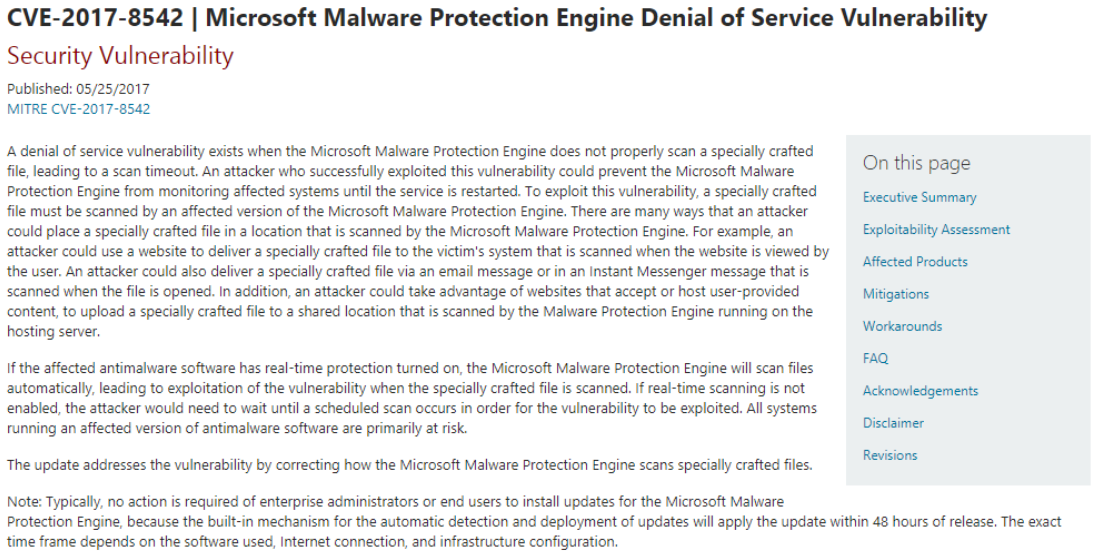
Underlying OS : Windows (Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016, Microsoft Exchange Server 2013 and 2016)

Dampak : Remote user dapat mengubah konten yang jika dimuat oleh pengguna target, akan mengeksekusi kode acak dengan local system privileges pada sistem target. User local dapat mencegah target untuk memantau sistem. Service restart sangat diperlukan untuk mengembalikan sistem ke normalnya.

Solusi : vendor yaitu Microsoft telah mengeluarkan sebuah perbaikan yaitu mengupdate atau memperbarui microsoft malware protection engine pada Microsoft windows defender dan Microsoft forefront

Microsoft menyatakan, jika potensi celah keamanan pada Windows Defender akan

lebih rendah pada Windows 10 dan 8.1 karena adanya fitur CFG yang mengamankan memory corruption.



CVE-2017-8542 | Microsoft Malware Protection Engine Denial of Service Vulnerability

Security Vulnerability

Published: 05/25/2017
MITRE CVE-2017-8542

A denial of service vulnerability exists when the Microsoft Malware Protection Engine does not properly scan a specially crafted file, leading to a scan timeout. An attacker who successfully exploited this vulnerability could prevent the Microsoft Malware Protection Engine from monitoring affected systems until the service is restarted. 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 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 antimalware software are primarily at risk.

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

Note: 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.

On this page

Executive Summary
Exploitability Assessment
Affected Products
Mitigations
Workarounds
FAQ
Acknowledgements
Disclaimer
Revisions

Vendor URL : portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8542

How to attack Windows Defender

Celah keamanan pada Windows Defender memungkinkan penyerang (hacker) dapat memasuki suatu sistem tanpa dibutuhkan interaksi dengan pengguna komputer. Metode yang digunakan penyerang, cukup dengan mengirim email atau pesan instan yang akan di-scan oleh Windows Defender. Jenis objek yang akan di-scan secara otomatis oleh Windows Defender seperti website dan file pun dapat dijadikan sebagai objek serangan.

Ahli riset di Google Project Zero yang menemukan celah keamanan pada Windows Defender, mengatakan exploit yang menyerang Windows Defender dapat menyebar seperti worm, yaitu membentuk rantai serangan yang berpindah dari komputer yang rentan ke komputer rentan lainnya.

Ancaman keamanan memanfatkan Windows Defender dapat dibilang serangan remote code execution terburuk yang ada. Hal tersebut dikarenakan, Windows Defender terinstal secara default, serangan tidak mesti dilakukan pada satu jaringan LAN dan dapat menyebar.

MsMpEng merupakan proses yang dieksploitasi oleh hacker dimana proses berjalan dengan hak akses tertinggi sehingga dampak serangan memiliki kemungkinan terburuk. Microsoft sendiri mengatakan jika mereka belum melihat eksploitasi nyata terhadap Windows Defender yang telah terjadi.

NScript merupakan komponen seperti JavaScripts yang terdapat pada MsMpEng yang bertujuan untuk menganalisa sistem dan aktifitas jaringan. NScript berjalan dengan hak akses tertinggi dan di luar sandbox namun digunakan untuk mengevaluasi kode berbahaya.

Eksploitasi dilakukan dengan beberapa baris kode JavaScript yang disisipi melalui halaman website, email atau objek serangan yang lain. Hal ini merupakan salah satu permasalahan terbesar bagi aplikasi antivirus yang berusaha memproteksi dari segala sisi namun semakin membuka kerentanan pada aplikasi. Metode eksploitasi dapat dilakukan melalui file zip, emulator ROM, file Python, melalui LAN dan lainnya.