Alert on Microsoft Malware Protection Engine Critical Vulnerability (CVE-2018-0986

Overview

Microsoft Malware Protection Engine (MMPE) is used to automatically scan all incoming files in Microsoft Anti-malware products.

Microsoft released a security update to address vulnerability in the Microsoft Malware Protection Engine that enables hacker to perform remote code execution.

A remote hacker could exploit this vulnerability in order to have access over affected system. Various methods such as sending a crafted malicious file as an email attachment or file sharing are been used. The vulnerable MMPE scans this malicious file, thereby corrupting the memory, which enables the hacker to execute arbitrary code on the system.

Affected Products

The following Microsoft products using MMPE version 1.1.14600.4 or prior are affected:

- Windows 7 for 32-bit Systems SP1 and x64-based Systems SP1
- Microsoft Windows 8.1 for 32-bit System and x64-based Systems
- Microsoft Windows RT 8.1
- Windows 10 for 32-bit Systems and x64-based Systems
- Windows 10 Version 1511 for 32-bit Systems and x64-based Systems
- Windows 10 Version 1607 for 32-bit Systems and x64-based Systems
- Windows 10 Version 1703 for 32-bit Systems and x64-based Systems
- Windows 10 Version 1709 for 32-bit Systems and x64-based Systems
- Windows Server 2008 for 32-bit Systems SP 2, x64-based Systems SP 2 and Itanium-based Systems SP2
- Windows Server 2008 R2 for x64-based Systems SP1 and Itanium-based Systems SP1

- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
- Windows Server 2008 R2 for x64-based Systems SP1 (Server Core installation)
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2 (Server Core installation)
- Windows Server 2016 (Server Core installation)
- Windows Server Version 1709 (Server Core installation)
- Microsoft Exchange Server 2013
- Microsoft Exchange Server 2016
- Microsoft Forefront Endpoint Protection 2010
- Microsoft Security Essentials
- Windows Intune Endpoint Protection

Recommendations

NITDA CERRT recommends that appropriate patches as mentioned in Microsoft Security Guidance should be applied.
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0986

References

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0986

https://www.bleepingcomputer.com/news/security/microsoft-out-of-band-security-update-patches-malware-protection-engine-flaw/

Contact Information

support@cerrt.ng
telephone line; (+234)-0800998877665544.