CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2021-001

Microsoft Defender Remote Code Execution Vulnerability

January 13, 2021 — v1.0

TLP:WHITE

History

- *13/01/2021 — v1.0 – Initial publication*

Summary

On 12th of January 2021, Microsoft released several security advisories to address security vulnerabilities. One of the reported vulnerabilities – a remote code execution – affects Microsoft Defender and is **actively exploited** in the wild [1, 3].

Technical Details

The vulnerability is being tracked as CVE-2021-1647 and received CVSS:3.0 - score of 7.8. It is a remote code execution (RCE) found in the Malware Protection Engine component (`mpengine.dll`) [2]. The threat actor could execute code on vulnerable devices by tricking a user into opening a malicious document on a system where Defender is installed [3].

According to Microsoft's exploitability assessment, the vulnerability is not publicly disclosed, but Microsoft is aware of instances of this vulnerability being exploited [1]. The technique is not functional in all situations, and is still considered to be at a proof-of-concept level. However, the code could evolve for more reliable attacks [3].

Affected Products

- First version of the Microsoft Malware Protection Engine with this vulnerability addressed - Version 1.1.17700.4
- Last version of the Microsoft Malware Protection Engine affected by this vulnerability - Version 1.1.17600.5 [1].

Recommendations

CERT-EU recommends to update to a version of Microsoft Malware Protection Engine, where this vulnerability has been addressed (1.1.17700.4 or later).

The default configuration in Microsoft antimalware software helps ensure that malware definitions and the Microsoft Malware Protection Engine are kept up to date automatically [1]. 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.

End users that do not wish to wait can manually update their antimalware software [1].

References

[1] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-1647

[2] https://www.bleepingcomputer.com/news/security/microsoft-patches-defender-antivirus-zero-day-exploited-in-the-wild/

[3] https://www.zdnet.com/article/microsoft-fixes-defender-zero-day-in-january-2021-patch-tuesday/