CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2021-042

Critical Vulnerability in Microsoft Hyper-V

July 29, 2021 — v1.0

TLP:WHITE

History:

- *29/07/2021 — v1.0 – Initial publication*

Summary

On May 11, Microsoft published a security update guide about a critical Hyper-V Remote Code Execution Vulnerability, tracked as `CVE-2021-28476` with a CVSS score of 9.9 [1]. The exploitation of this vulnerability can lead to denial of service conditions or remote code execution [2]. A proof of concept for this vulnerability is now publicly available [3].

Technical Details

The vulnerability `CVE-2021-28476` relies on Hyper-V's virtual switch (*vmswitch*) that does not validate the value of an object identifier request that is intended for a network adapter.

Attackers need to have access to a guest virtual machine to exploit this vulnerability, and from there, send a specially crafted packet to the Hyper-V host. The exploitation of this vulnerability can lead to the crash of the host, or to remote code execution on the host and on the virtual machines attached to it. [2]

Affected Products

- Windows Server 2012 R2 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 (Server Core installation)
- Windows Server 2012
- Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
- Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 for x64-based Systems Service Pack 2
- Windows 8.1 for x64-based systems
- Windows 7 for x64-based Systems Service Pack 1
- Windows Server 2016 (Server Core installation)
- Windows Server 2016
- Windows 10 Version 1607 for x64-based Systems

- Windows 10 for x64-based Systems
- Windows Server, version 20H2 (Server Core Installation)
- Windows 10 Version 20H2 for x64-based Systems
- Windows Server, version 2004 (Server Core installation)
- Windows 10 Version 2004 for x64-based Systems
- Windows Server, version 1909 (Server Core installation)
- Windows 10 Version 1909 for x64-based Systems
- Windows Server 2019 (Server Core installation)
- Windows Server 2019
- Windows 10 Version 1809 for x64-based Systems
- Windows 10 Version 1803 for x64-based Systems

Recommendations

Microsoft recommends to apply Monthly Rollup or Security Update depending on the running version of Windows. [1]

CERT-EU also recommends updating the vulnerable systems as soon as possible.

References

[1] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-28476

[2] https://www.bleepingcomputer.com/news/security/critical-microsoft-hyper-v-bug-could-haunt-orgs-for-a-long-time/

[3] https://github.com/0vercl0k/CVE-2021-28476