CERT-EU

Security Advisory 2022-016

Important Vulnerability in Windows SMBv3

March 10, 2022 — v1.0

TLP:WHITE

History:

- *10/03/2022 — v1.0 – Initial publication*

Summary

On March 8th, Microsoft fixed in the monthly Patch Tuesday 71 vulnerabilities with three classified as **Critical** as they allow remote code execution [1]. A remote code execution vulnerability classified as **Important** affects Windows SMBv3 Client/Server.

The vulnerability tracked as CVE-2022-24508 is a remote code execution vulnerability allowing an authenticated user to execute malicious code on Windows 10 version 2004 and newer systems via SMBv3 [2]. No active exploitation of this vulnerability is known yet.

Technical Details

There is not much detail available about how this vulnerability could be exploited. However, it is notable because it is listed as *Exploitation more likely* by Microsoft. This vulnerability is rated **Important** rather than **Critical**. There is no public disclosure, and it is not currently being exploited. However, the attack vector and likelihood of exploitation make it a candidate for possible attacks, and so this should be a high priority for patching [3].

Affected Products

- Windows 10 Version 21H1 for 32-bit Systems
- Windows 10 Version 21H1 for ARM64-based Systems
- Windows 10 Version 21H1 for x64-based Systems
- Windows 10 Version 20H2 for 32-bit Systems
- Windows 10 Version 20H2 for x64-based Systems
- Windows Server 2022 Azure Edition Core Hotpatch
- Windows Server 2022 (Server Core installation)
- Windows Server 2022
- Windows 10 Version 21H2 for x64-based Systems
- Windows 10 Version 21H2 for ARM64-based Systems
- Windows 10 Version 21H2 for 32-bit Systems
- Windows 11 for ARM64-based Systems

- Windows 11 for x64-based Systems
- Windows Server, version 20H2 (Server Core Installation)
- Windows 10 Version 20H2 for ARM64-based Systems

Mitigations

Microsoft strongly recommends to install the updates but also provide workaround steps by disabling SMBv3 compression [4].

Recommendations

CERT-EU recommends to apply the patches released on March 2022 Patch Tuesday [5].

References

[1] https://www.bleepingcomputer.com/news/microsoft/microsoft-march-2022-patch-tuesday-fixes-71-flaws-3-zero-days/

[2] https://www.theregister.com/2022/03/09/microsoft_patch_tuesday/

[3] https://news.sophos.com/en-us/2022/03/08/microsoft-patches-71-vulnerabilities-including-rdp-client-exchange-server-intune/

[4] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24508

[5] https://msrc.microsoft.com/update-guide/releaseNote/2022-Mar