10 years CERT-EU

Security Advisory 2022-026

Critical Vulnerabilities in Microsoft Windows

April 13, 2022 — v1.0

TLP:WHITE

History:

- *13/04/2022 — v1.0 – Initial publication*

Summary

On April 12th, Microsoft issued the monthly Patch Tuesday where 128 vulnerabilities were fixed [1]. Three of them were classified as **Critical** as they allow remote code execution (RCE) with no user interaction. Two other vulnerabilities rated as important can be used for privilege escalation, but since one of them is already being actively exploited and the other has a public exploit, we recommend to patch all of them as soon as possible.

Technical Details

The vulnerability tracked as CVE-2022-26809 - CVSS score: 9.8 - is a remote procedure call runtime RCE vulnerability identified in Microsoft's Server Message Block (SMB) functionality. By sending a crafted remote procedure call (RPC) to an RPC host machine, an attacker can obtain remote code execution on the server side with the same permissions as the RPC service [2].

The two vulnerabilities CVE-2022-24491 and CVE-2022-24497 - CVSS score: 9.8 - have been identified in Windows Network File System and the result of the exploitation can also lead to RCE. Microsoft detailed that on systems where the NFS role is enabled, a remote attacker could execute their code on an affected system with high privileges and without user interaction [3, 4].

The vulnerability tracked as CVE-2022-24521 - CVSS score: 7.8 - is a Windows Common Log File System Driver Execution Vulnerability that can be used for privilege escalation by an attacker that is already logged in into the machine. **It is already being actively exploited** [5].

The second privilege escalation vulnerability is tracked as CVE-2022-26904 - CVSS score: 7.0 - and it was found in the Windows User Profile Service. Successful exploitation of this vulnerability requires an attacker to win a race condition. No active exploitation of this vulnerability is known yet, but an exploit has been made public [6].

Affected Products

These vulnerabilities can be found in most of the Microsoft Windows releases starting with Windows 7 until Windows Server 2022.

Please refer to the links provided for each vulnerability in order to identify the exact versions of each affected system and the patch that should be applied.

Recommendations

We strongly advise to apply the patch as soon as possible.

For CVE-2022-26809, Microsoft recommends configuring firewall rules to help prevent this vulnerability from being exploited; TCP port 445 can be blocked at the network perimeter [7].

References

[1] https://msrc.microsoft.com/update-guide/releaseNote/2022-Apr

[2] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26809

[3] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24491

[4] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24497

[5] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-24521

[6] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-26904

[7] https://docs.microsoft.com/en-gb/windows-server/storage/file-server/smb-secure-traffic