Security Advisory 2023-020

Remote Code Execution vulnerability in Windows HTTP protocol stack

March 15, 2023 — v1.0

TLP:CLEAR

History:

- *15/03/2023 — v1.0 – Initial publication*

Summary

On March 14, 2023, Microsoft released a security fix for a vulnerability (`CVE-2023-23392`) in the HTTP/3 protocol stack of Microsoft Windows Server 2022 and Windows 11 systems [1]. This vulnerability allows a remote attacker to execute arbitrary code. Microsoft expects this vulnerability likely to be exploited soon.

Technical Details

The vulnerability exists in the HTTP/3 protocol stack of current Microsoft Windows systems. An attacker can exploit this vulnerability if the attacked system fulfils some prerequisites:

- HTTP/3 needs to be active, and
- the server uses buffered I/O.

If the system fulfils these prerequisites, an attacker can send a specially crafted packet to the system and trigger the vulnerability.

Affected Products

Microsoft Windows Server 2022, Microsoft Windows 11 (21H2,22H2).

Recommendations

CERT-EU strongly recommends applying the latest patches for Microsoft Windows Server 2022, focusing on Internet-facing systems first. Additionally, CERT-EU recommends applying the latest patches to systems running Microsoft Windows 11.

Mitigations

HTTP/3 support for services is a new feature in recent Windows operating systems. A prerequisite for a server to be vulnerable is that the binding has HTTP/3 enabled, and the server uses buffered I/O. Therefore, disabling HTTP/3 via a registry key mitigates this vulnerability [2].

References

[1] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-23392

[2] https://techcommunity.microsoft.com/t5/networking-blog/enabling-http-3-support-on-windows-server-2022/ba-p/2676880