Security Advisory 2025-040

Critical Vulnerability in Windows Server Update Service (WSUS)

2025-10-24 — v1.0

TLP:CLEAR

History:

- *24/10/2025 — v1.0 – Initial publication*

Summary

On October 23, 2025, Microsoft released an out-of-band update to address a critical vulnerability in Windows Server Update Service (WSUS). This vulnerability could allow a remote unauthenticated attacker to execute code on the targeted systems [1]. A proof-of-concept is publicly available for this vulnerability [2].

It is recommended to update as soon as possible.

Technical Details

The vulnerability **CVE-2025-59287**, with a CVSS score of 9.8, is an unsafe deserialisation issue that may allow a remote, unauthenticated attacker to execute malicious code on affected assets with SYSTEM privileges.

Affected Products

This vulnerability affects Microsoft Windows Server with the WSUS server role enabled. Microsoft published an update for the following versions of Windows Server:

- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- Windows Server 23H2
- Windows Server 2025

Recommendations

It is recommended to update affected assets as soon as possible.

References

[1] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-59287

[2] https://hawktrace.com/blog/CVE-2025-59287