CERT-EU

Security Advisory 2026-007

Critical Vulnerability in Windows Netlogon

2026-05-10 — v1.0

TLP:CLEAR

History:

- *10/06/2026 — v1.0 – Initial publication*

Summary

On 12 May 2026, Microsoft published a security advisory addressing a critical vulnerability affecting Windows Server when acting as a domain controller [1]. This vulnerability allows an unauthenticated attacker to execute arbitrary code over a network.

According to The Centre for Cybersecurity Belgium (CCB), this vulnerability is currently exploited by threat actors [2]. It is strongly recommended updating affected Windows servers as soon as possible.

Technical Details

The vulnerability **CVE-2026-41089**, with the CVSS score of 9.8, is a stack-based buffer overflow in Windows Netlogon [1].

An unauthenticated attacker could execute arbitrary code with SYSTEM privileges on targeted domain controllers by sending specially crafted packets [3].

Affected Products

The following Windows Server versions are affected:

- Windows Server 2012 / 2012 R2
- Windows Server 2016 (prior to 10.0.14393.9140)
- Windows Server 2019 (prior to 10.0.17763.8755)
- Windows Server 2022 (prior to 10.0.20348.5074)
- Windows Server 2022 23H2 (prior to 10.0.25398.2330)
- Windows Server 2025 (prior to 10.0.26100.32772)

Additional information is available in the vendor's advisory [1].

Recommendations

It is recommended updating affected Windows Server asset as soon as possible.

References

[1] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-41089

[2] https://ccb.belgium.be/advisories/warning-microsoft-patch-tuesday-may-2026-patches-118-vulnerabilities-16-critical-102#:~:text=It%20is%20now%20actively%20exploited%20in%20the%20wild

[3] https://www.bleepingcomputer.com/news/microsoft/critical-windows-netlogon-remote-code-execution-flaw-now-exploited-in-attacks/