

Forum:[Hack Forums](#)

Thread: [Critical Windows Netlogon RCE flaw now exploited in attacks](#)

MadScientist - June 1, 2026, 9:25 am

The Centre for Cybersecurity Belgium (CCB), the country's national authority for cybersecurity, warned on Friday that threat actors are now exploiting a recently patched critical Windows Netlogon vulnerability in attacks.

Netlogon is a remote procedure call (RPC) interface and a core Microsoft Windows Server background service that authenticates services and users on Windows domain-based networks.

Microsoft patched this vulnerability (CVE-2026-41089) during the May 2026 Patch Tuesday, describing it as a stack-based buffer overflow in Windows Netlogon that allows attackers without privileges to gain remote code execution on targeted domain controllers.

"An attacker could send a specially crafted network request to a Windows server that is acting as a domain controller," it said. "If successful, this could cause the Netlogon service to improperly handle the request, potentially allowing the attacker to run code on the affected system without needing to sign in or have prior access."

CVE-2026-41089 impacts all currently supported Windows Server versions, including the latest release, Windows Server 2025.

According to a security advisory published by the company on May 12, the vulnerability was discovered by Windows Attack Research & Protection (WARP), an internal offensive cybersecurity and engineering research team at Microsoft.

On Friday, Belgium's national cybersecurity authority (CCB) warned that attackers are now actively exploiting the CVE-2026-41089 security flaw in the wild and urged admins to immediately patch vulnerable servers.

"CVE-2026-41089 in #Windows #Netlogon is now actively #exploited in the wild and could lead to #RCE. CVSS(3.1): 9.8," the CBC warned in a Friday tweet. "Patch as quickly as possible."

Read More -

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

The Pact - June 1, 2026, 10:55 pm

All supported Windows' Server versions acting as domain controllers are reported affected; Microsoft's updates cover multiple server releases. Unpatched domain controllers reachable over the network are the primary high-value targets. So that's a problem.