Microsoft confirms NTLM authentication failures after November Windows updates



Microsoft says November security updates for CVE-2026-118737 can break NTLM authentication with some third-party proxies, SSO and packaging tools. No fix exists yet; a temporary registry workaround is available.

- CVE-2026-118737 is a high-severity remote code execution flaw in the Windows Remote Procedure Call Runtime, exploitable by unauthenticated attackers without user interaction on unpatched systems.
- The November updates are the first phase of NTLM message-signing improvements intended to reduce relay-attack exposure.
- Some third-party authentication proxies, SSO solutions and application packaging tools that implement NTLM incorrectly may fail to authenticate on patched devices.

> - No fix is available yet; the ClientAllowUnsignedNtlm registry value is a short-term workaround that Microsoft may remove.
> - Microsoft is also tracking activation failures, SQL Server performance issues and a printing problem linked to this month's updates.

Microsoft has confirmed that its November security updates, which address CVE-2026-118737, may cause authentication failures on patched devices. The vulnerability is a high-severity remote code execution flaw in the Windows Remote Procedure Call Runtime, caused by a timing-dependent authentication weakness. Unauthenticated attackers can exploit it remotely, without user interaction, on unpatched systems.

What is going wrong

The updates are the first phase of NTLM message-signing improvements. They ensure that authenticated NTLM sessions always establish a cryptographic session key and negotiate real message signing, which reduces exposure to relay attacks. Microsoft says some third-party apps and devices, including authentication proxy servers, single sign-on solutions and application packaging tools using NTLM, are affected when they do not implement the protocol correctly. One example is a device that sets a target-info flag in its challenge message but supplies an empty or incomplete TargetInfo field.

Affected devices return an NTLMSSP_CHALLENGE message with an empty Target Info List in network traces, or show Target Machine values of "Not Found" in event logs. No fix is available yet.

Microsoft's guidance

As a temporary measure, Microsoft suggests setting the ClientAllowUnsignedNtlm registry value under the MSV1_0 key to 1. It also advises checking whether the device or application can use Kerberos, or whether the vendor offers an update compatible with the new signing requirements, and otherwise asking the vendor for a compliant update. Microsoft describes the registry setting as short-term and says it may be removed. Updating the product or using a compatible authentication configuration is the recommended long-term resolution.

Separately, Microsoft has confirmed activation failures and SQL Server performance issues tied to this month's updates, and is investigating a printing issue with complex documents.

What to do now

1. Do not defer the November updates broadly; CVE-2026-118737 is a high-severity remote code execution flaw, so pilot them and roll out in stages.
2. Inventory NTLM-dependent proxies, SSO solutions and application packaging tools, and test them against patched endpoints before wide deployment.
3. Look for the symptoms Microsoft describes: empty Target Info List in NTLMSSP_CHALLENGE traces and

"Not Found" Target Machine values in event logs.

4. Ask affected vendors for NTLM-compliant updates, and assess moving those systems to Kerberos where supported.
5. If you use the ClientAllowUnsignedNtlm workaround, limit it to affected systems, record it as a time-bound exception in change and risk registers, and plan its removal.