Microsoft Lists CVE-2026-84015, a Remote Code Execution Flaw in Windows PPP EAP-TLS



Microsoft's MSRC has published CVE-2026-84015, a remote code execution vulnerability in Remote Access Point-to-Point Protocol (PPP) EAP-TLS. The latest update only revises an acknowledgement.

- The vulnerability is tracked as CVE-2026-84015.
- It affects Remote Access Point-to-Point Protocol (PPP) EAP-TLS and is classed as remote code execution.
- The latest revision updates an acknowledgement and is informational only.
- The source excerpt gives no severity score, affected versions or patch details.

Microsoft's Security Response Center has listed CVE-2026-84015, described as a Remote Access Point-to-Point

Protocol (PPP) EAP-TLS Remote Code Execution Vulnerability.

What the source says

The entry identifies the issue as a remote code execution vulnerability in the PPP EAP-TLS component used for remote access. The most recent change to the page updates an acknowledgement. Microsoft describes this as an informational change only, so the update does not by itself signal a change in the technical assessment.

What is not stated

The excerpt we reviewed does not include a severity score, the list of affected Windows versions, exploitation status, or the fix. We therefore cannot say which systems are exposed or how urgent patching is. Those details should be taken directly from the Microsoft update guide entry.

Why it matters

Remote code execution in a remote access component deserves attention from teams that run Windows-based VPN or remote access services, particularly where EAP-TLS is used for authentication. Institutions should confirm whether they use this feature before deciding on priority.

A measured response is to review the full MSRC entry, map it to your asset inventory, and schedule the vendor fix through your normal change process, accelerating it if the entry indicates active exploitation or a high score.

What to do now

1. Read the full CVE-2026-84015 entry in the Microsoft update guide for affected versions, score and fix.
2. Check your asset inventory for Windows systems providing remote access with PPP and EAP-TLS.
3. Schedule the Microsoft security update through change management, prioritising internet-facing systems.
4. Review exposure of remote access services and restrict it to what is necessary until patched.
5. Record the assessment and decision for your vulnerability management evidence.