Microsoft lists CVE-2026-72965, a Windows WebClient Service privilege escalation flaw



Microsoft has published an entry for CVE-2026-72965, an elevation of privilege vulnerability in the Windows WebClient Service. The latest revision only updates an acknowledgement and changes nothing technical.

- The vulnerability is tracked as CVE-2026-72965.
- It affects the Windows WebClient Service and is classed as elevation of privilege.
- The latest revision is informational only and updates an acknowledgement.
- The excerpt provided does not state severity scores, affected versions or patch details.

What was published

Microsoft's Security Response Center has an entry for CVE-2026-72965, described as an elevation of privilege vulnerability in the Windows WebClient Service. Elevation of privilege flaws generally allow a user or process to gain rights beyond those it was granted.

The most recent change to the entry is described as informational only: an acknowledgement was updated. The notice does not indicate any change to the vulnerability itself, its rating or its remediation.

What the source does not say

The material available to us does not give a severity score, the list of affected Windows versions, exploitation status or the specific security update that addresses the issue. We therefore make no claims on those points.

What this means for your institution

There is no need for alarm based on this revision alone. The sensible step is to open the full Microsoft entry, confirm whether your Windows estate is affected, and handle the fix through your normal patch management process, prioritised according to the details Microsoft provides.

What to do now

1. Read the full CVE-2026-72965 entry on the Microsoft Update Guide and note affected versions and the fix.
2. Check your asset inventory for Windows systems where the WebClient Service is present or running.
3. Schedule the relevant Microsoft update through your standard patch process, prioritising by the severity Microsoft assigns.
4. Record the assessment and decision in your vulnerability management log for audit purposes.