Microsoft lists CVE-2026-69370, a remote code execution flaw in Visual Studio Code



Microsoft's update guide lists CVE-2026-69370, a remote code execution vulnerability in Visual Studio Code. The latest revision only updates an acknowledgement and is informational.

- The vulnerability is tracked as CVE-2026-69370 and affects Visual Studio Code.
- Microsoft classifies it as a remote code execution vulnerability.
- The latest revision updates an acknowledgement and is described as informational only.
- The excerpt provided does not state severity scores, affected versions or fixes.

Microsoft's Security Response Center has published an entry in its update guide for CVE-2026-69370, described as a remote code execution vulnerability in Visual Studio Code.

What the entry says

The most recent revision updates an acknowledgement. Microsoft states that this is an informational change only, so it does not signal a change in the technical content of the advisory. The excerpt available to us does not include a severity rating, the affected versions, exploitation status or remediation details.

Why it matters

Visual Studio Code is widely used by development and engineering teams, often on workstations with access to source code, credentials and internal systems. A remote code execution issue in a developer tool therefore deserves a place in normal vulnerability triage, even while details are limited.

Suggested approach

Treat the full Microsoft entry as the authoritative source. Confirm whether Visual Studio Code is installed in your environment, check the guidance on the MSRC page, and apply any update Microsoft lists through your normal change process. No further action is implied by the informational revision itself.

What to do now

1. Inventory where Visual Studio Code is installed, including developer and administrator workstations.
2. Read the full CVE-2026-69370 entry on the Microsoft update guide for affected versions and fixes.
3. Apply the Microsoft-listed update through your standard patch and change management process.
4. Record the item in your vulnerability register with the owner and review date.