CVE-2026-87697: Microsoft Lists a .NET Remote Code Execution Vulnerability



Microsoft's update guide lists CVE-2026-87697, a remote code execution vulnerability in .NET. The latest revision only updates an acknowledgement and does not change the technical content.

- The entry is titled CVE-2026-87697 .NET Remote Code Execution Vulnerability.
- The vendor describes the vulnerability class as remote code execution in .NET.
- The latest revision updated an acknowledgement and is informational only.
- The source excerpt gives no severity score, affected versions or patch details.

Microsoft's Security Response Center has published an entry for CVE-2026-87697, described as a .NET remote code execution vulnerability. The most recent revision updated an acknowledgement. Microsoft labels this an

informational change, so it does not signal any change in the technical guidance.

What the source states

The material available to us is limited. It confirms the CVE identifier, the product family (.NET) and the vulnerability class (remote code execution). It does not state a severity rating, the affected versions, exploitation status or the fixed builds.

What this means for your organisation

Because the details are not in the excerpt, the right step is to read the full entry in Microsoft's update guide and map it against your own estate. Remote code execution flaws in a widely used runtime deserve prompt triage, but any urgency should follow what the full advisory says rather than assumptions.

The acknowledgement update does not by itself require action. If your team already reviewed this entry, there is no new reason to reopen it on account of this revision.

Suggested next steps

- Open the official entry and record the severity, affected versions and available fixes.
- Check your asset and application inventory for .NET runtimes and applications built on them.
- Schedule patching through your normal change process, prioritising internet-facing systems once the advisory confirms what applies.

What to do now

1. Read the full Microsoft entry and record severity, affected versions and fixes.
2. Identify .NET runtimes and dependent applications in your asset inventory.
3. Prioritise internet-facing .NET systems for assessment once applicability is confirmed.
4. Patch through your standard change process and document the outcome.