Microsoft Lists CVE-2026-70174, a .NET Remote Code Execution Vulnerability



Microsoft's Security Response Center has an entry for CVE-2026-70174, a .NET remote code execution vulnerability. The latest update only revised an acknowledgement and changes nothing technical.

- The vulnerability is tracked as CVE-2026-70174 and described as a .NET remote code execution issue.
- The entry sits in Microsoft's MSRC Update Guide.
- The latest revision updated an acknowledgement and is described as informational only.
- The visible source text gives no severity score, affected versions or patch details.

Microsoft's Security Response Center (MSRC) lists CVE-2026-70174 in its Update Guide as a .NET remote code

execution vulnerability.

What changed

The most recent revision of the entry updated an acknowledgement. Microsoft describes this as an informational change only, so the update does not signal a change in the nature of the issue or in the guidance.

What the source does not say

The text available to us does not include a severity rating, the affected .NET versions, exploitation status or the fix. We therefore make no claims on those points. Teams should read the full MSRC entry for the authoritative details before deciding on priority.

Practical view

Because .NET is widely used in internal and customer-facing applications, it is worth confirming where it runs in your estate and who owns each application. Remote code execution flaws in a common runtime are normally handled through the vendor's patch process, so the entry should be routed into your existing vulnerability and change management workflow.

The acknowledgement change itself needs no separate action. The value of the entry lies in the vulnerability record it points to.

What to do now

1. Open the MSRC entry for CVE-2026-70174 and record the severity, affected versions and fix details.
2. Identify applications and servers running .NET, including third-party software that bundles it.
3. Add the CVE to your vulnerability register with an owner and a priority based on the MSRC details.
4. Schedule patching through normal change management once the fix applies to your versions.