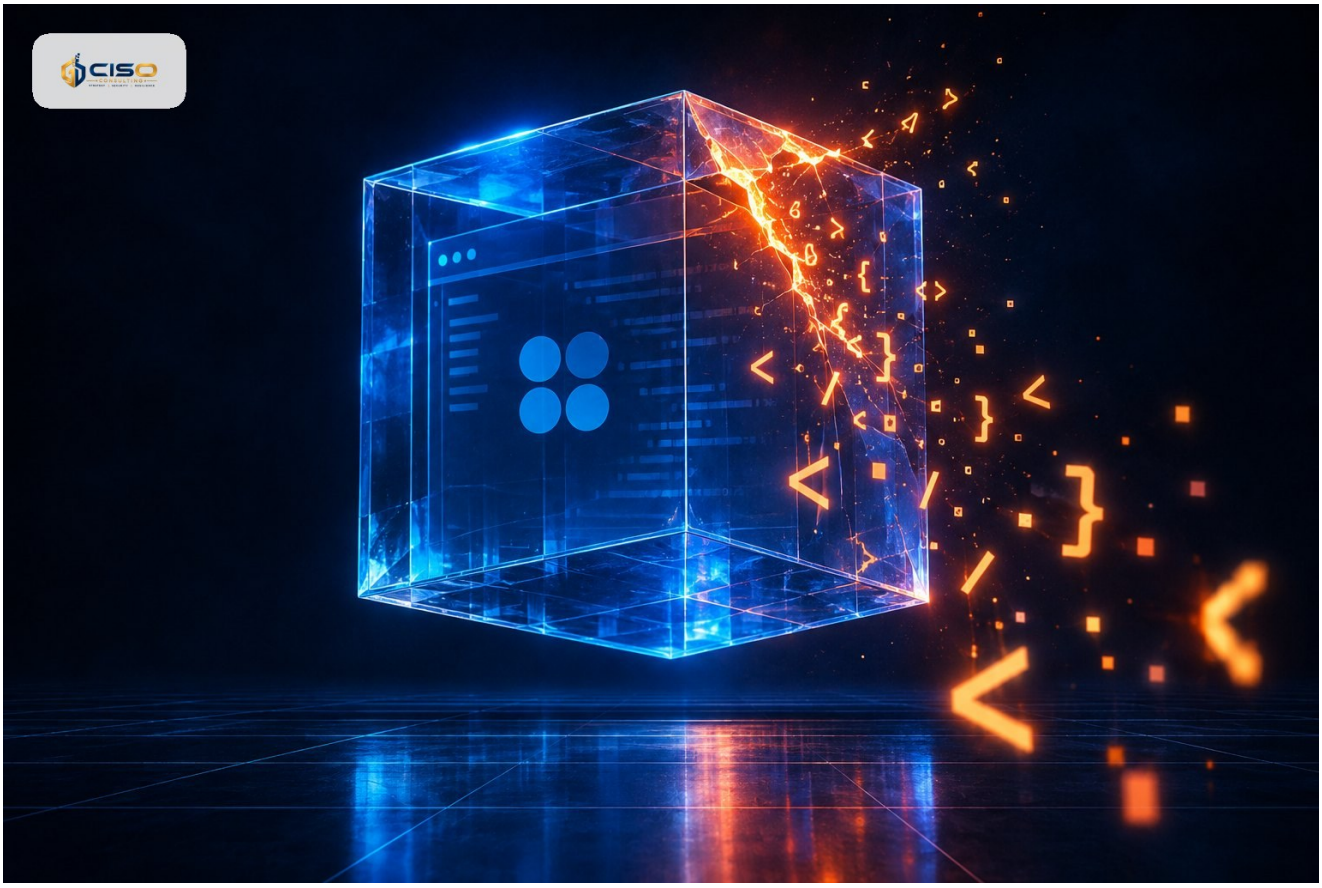
# Microsoft Lists CVE-2026-70197, a Remote Code Execution Flaw in .NET and Visual Studio



Microsoft's MSRC lists CVE-2026-70197, a remote code execution vulnerability affecting .NET and Visual Studio. The latest revision only updates an acknowledgement and changes no technical content.

- CVE-2026-70197 is classed as a remote code execution vulnerability in .NET and Visual Studio.
- The entry was updated only to revise an acknowledgement; Microsoft describes this as an informational change.
- The source extract gives no severity score, affected versions or patch details.
- Organisations should consult the MSRC Update Guide entry for the authoritative details.

Microsoft's Security Response Center has published an entry for CVE-2026-70197, titled as a .NET and Visual

Studio Remote Code Execution Vulnerability. The most recent change to the entry updates an acknowledgement. Microsoft states that this is an informational change only.

## What the source tells us

The available text confirms the CVE identifier, the affected products (.NET and Visual Studio) and the vulnerability class, remote code execution. It does not state a severity rating, the affected versions, exploitation status or the fixed builds. We therefore make no claims on those points.

## What it means for your organisation

.NET and Visual Studio are widely used in internal application development and in build environments. A remote code execution issue in such components is worth tracking even when the latest revision is informational, because the underlying entry may carry guidance that applies to your estate.

The revision itself does not signal a change in risk. It does, however, offer a sensible prompt to confirm that your teams have reviewed the full entry and know whether any of your systems are in scope.

## Recommended approach

Treat this as a verification task rather than an emergency. Read the MSRC entry directly, match it against your asset inventory, and follow Microsoft's remediation guidance through your normal change process.

## What to do now

1. Read the full CVE-2026-70197 entry in the MSRC Update Guide for affected versions and fixes.
2. Check your asset inventory for .NET runtimes and Visual Studio installations, including developer workstations and build servers.
3. Apply Microsoft's remediation through your standard patch and change-management process once scope is confirmed.
4. Record the assessment outcome in your vulnerability management register.