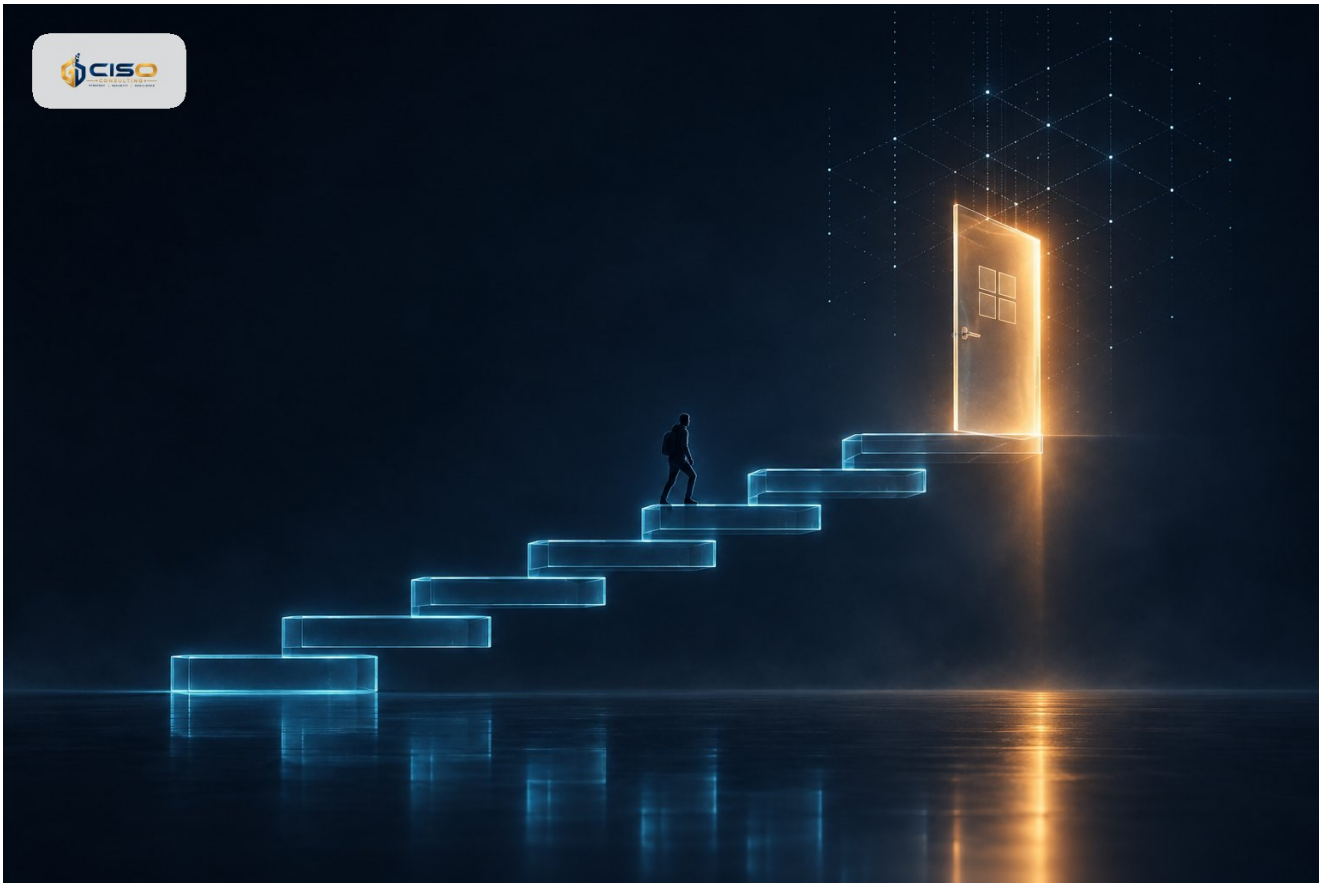
Microsoft Lists CVE-2026-109481, an ASP.NET Core Elevation of Privilege Flaw



Microsoft's MSRC has an entry for CVE-2026-109481, an elevation of privilege vulnerability in ASP.NET Core. The latest update only changes an acknowledgement and is informational.

- The vulnerability is tracked as CVE-2026-109481 and affects ASP.NET Core.
- Microsoft classifies it as an elevation of privilege vulnerability.
- The latest revision updates an acknowledgement only and is described as informational.
- The source excerpt gives no severity score, affected versions or patch details.

What was published

Microsoft's Security Response Center lists CVE-2026-109481 in its update guide as an elevation of privilege

vulnerability in ASP.NET Core. The most recent revision to the entry changes an acknowledgement. Microsoft describes this change as informational, so it does not signal a change in the technical assessment.

What the source does not say

The material available to us does not state a severity rating, the affected versions, the conditions needed for exploitation, or whether exploitation has been observed. It also does not describe the fix. We therefore avoid drawing conclusions on risk and recommend reading the full MSRC entry directly.

What this means for your organisation

Elevation of privilege flaws matter because they can let an account or process gain more access than intended. Institutions that run web applications or APIs on ASP.NET Core should confirm whether they are in scope and what the vendor guidance says. This is a routine check rather than an emergency, until the full entry indicates otherwise.

For regulated entities, the item is a useful prompt to confirm that vulnerability and patch management processes capture vendor advisories for application frameworks, not only operating systems and network devices.

What to do now

1. Check your application inventory for ASP.NET Core workloads, including internally developed and third-party applications.
2. Read the full MSRC entry for CVE-2026-109481 to confirm affected versions and the available update.
3. Schedule any required update through your normal change and patch management process, prioritised by exposure.
4. Record the review outcome as evidence for your vulnerability management controls.