Critical flaw in legacy ASP.NET anti-CSRF library Idunno.AntiCsrf is under active exploitation



Researchers urge users to stop using the legacy Idunno.AntiCsrf library after a critical flaw, CVE-2026-131914 (CVSS 9.3), was exploited in the wild. Versions 0.9.1.0 and 0.9.1 Beta are affected.

- The affected component is Idunno.AntiCsrf (Idunno.AntiCsrf.dll), a legacy ASP.NET anti-CSRF library.
- The flaw is tracked as CVE-2026-131914 and scores 9.3 out of 10.0 on CVSS.
- Versions 0.9.1.0 and 0.9.1 Beta are affected.
- The vulnerability has been exploited in the wild.
- The headline describes the impact as unauthenticated remote code execution; researchers advise discontinuing use of the library.

Researchers have advised organisations to stop using Idunno.AntiCsrf, a legacy anti-CSRF library for ASP.NET, after a critical vulnerability in it was exploited in the wild.

What is known

The flaw is tracked as CVE-2026-131914 and carries a CVSS score of 9.3 out of 10.0. It affects versions 0.9.1.0 and 0.9.1 Beta of the library, which ships as Idunno.AntiCsrf.dll. The report's headline describes the impact as unauthenticated remote code execution. The excerpt available to us does not describe the technical mechanism, the exploitation activity, or whether a patched version exists, so those points should be confirmed against the full report and the maintainer's guidance.

Why it matters

Anti-CSRF libraries sit in the request path of web applications, and older ASP.NET applications may still reference this one without it being widely known. A critical flaw that is already being exploited, and that needs no authentication, raises the priority of finding every application that uses it, including internal and vendor-supplied ones.

What to do next

Start with an inventory, then decide between removal and replacement. Because researchers recommend discontinuing the library rather than simply updating it, plan for migration to a maintained alternative.

What to do now

1. Search application code, build artifacts and servers for Idunno.AntiCsrf.dll and identify versions 0.9.1.0 and 0.9.1 Beta.
2. Ask software vendors and internal development teams whether their ASP.NET applications use the library.
3. Plan removal or replacement with a maintained anti-CSRF mechanism, and check the maintainer's guidance for any fix.
4. Review web server and application logs on affected systems for suspicious activity, and escalate through incident response if found.
5. Record the finding in vulnerability and third-party component registers, and report significant exposure under your internal escalation process.