Unpatched Idunno AntiCsrf Flaw (CVE-2026-131914) Exploited for Remote Code Execution



Attackers are exploiting CVE-2026-131914 (CVSS 9.3), an insecure deserialization flaw in the abandoned Idunno AntiCsrf module for ASP.NET WebForms. No patch exists, and likely none will; affected sites should replace the library.

- CVE-2026-131914 (CVSS 9.3) is an insecure deserialization bug in how the library handles HTTP POST requests to ASP.NET WebForms endpoints.
- A single unauthenticated POST request, with no valid CSRF token, is enough; Mandiant reports exploitation in the wild.
- Code runs in the context of the IIS worker process, which can lead to full server compromise.
- The library has no maintainer; its last release, 0.9.1 Beta, dates from December 2008, and no official patch is available.

> - CISA added the flaw to its Known Exploited Vulnerabilities list and set a three-day deadline for US federal agencies.

Threat actors are exploiting an unpatched vulnerability in Idunno AntiCsrf, an open source anti-CSRF module for ASP.NET WebForms applications. The module has no active maintainer, and its most recent version, 0.9.1 Beta, was released in December 2008.

What is happening

The flaw, tracked as CVE-2026-131914 with a CVSS score of 9.3, is an insecure deserialization issue. According to WatchTowr, the library does not sufficiently check data from incoming form submissions before rebuilding it into program objects. Mandiant says an attacker needs only one HTTP POST request, with no authentication and no valid CSRF token, supplying a non-empty CSRF cookie value and a Base64-encoded gadget chain.

Because the vulnerable check runs before the application's own page logic, it can affect many pages on a site, not only those with login forms. Successful exploitation gives the attacker control of the IIS worker process, which can lead to full server compromise. Mandiant has observed active exploitation, and WatchTowr has seen exploit probes against its honeypots.

CISA added the flaw to its Known Exploited Vulnerabilities list and asked US federal agencies to address it within three days.

What to do

No official patch exists, and WatchTowr's researcher expects none. Organizations should stop using the module and move to an actively supported alternative. Where replacement is not immediately possible, WAF rules can serve as a stopgap until other workarounds are found. In parallel, teams should identify affected products and review audit logs for signs of exploitation.

What to do now

1. Inventory ASP.NET WebForms applications, including vendor-supplied products, to find any that package the Idunno.AntiCSRF library.
2. Replace the library with an actively supported anti-CSRF solution, and ask vendors of affected products for a replacement timeline.
3. Where replacement is not immediate, deploy WAF rules in front of affected applications as a temporary measure.
4. Review web server and application audit logs for signs of exploitation, and treat any suspected compromise of an IIS host as an incident.
5. Record the issue in the vulnerability and third-party risk registers, noting that no patch is expected.