CISA flags Idunno AntiCsrf deserialization flaw allowing remote code execution (CVE-2026-131914)



CISA lists CVE-2026-131914, a deserialization flaw in Idunno AntiCsrf that lets an unauthenticated remote attacker run arbitrary code. The product may be end-of-life; users should apply vendor mitigations or stop using it.

- CVE-2026-131914 is a deserialization of untrusted data flaw in Idunno AntiCsrf.
- An unauthenticated remote attacker can execute arbitrary code through object injection.
- The affected product may be end-of-life or end-of-service.
- Users are advised to stop using it or move to a supported version.
- CISA's federal due date is 2026-11-27; stakeholders must assess each asset's internet exposure.

What was reported

CISA has listed CVE-2026-131914, a deserialization of untrusted data vulnerability in Idunno AntiCsrf. According to the entry, an unauthenticated remote attacker can use object injection to execute arbitrary code. No authentication is needed, which is what makes the flaw significant for any exposed application.

The entry also notes that the affected product could be end-of-life or end-of-service. Where that is the case, users are advised to discontinue use or move to a supported version.

What CISA asks for

The required action is to apply mitigations in line with the vendor's instructions, and to follow CISA's BOD 26-04 guidance on prioritizing security updates based on risk, together with its Forensics Triage Requirements. For cloud services, the applicable BOD 26-04 guidance should be followed. If no mitigations are available, the product should no longer be used. Stakeholders are responsible for evaluating the internet exposure of each asset. The federal due date is 2026-11-27.

Practical reading for Saudi institutions

The BOD and due date apply to US federal bodies, but the logic carries over. Institutions should first establish whether any application or third-party component they run includes Idunno AntiCsrf, then judge how exposed those systems are. Where the component cannot be mitigated or is no longer supported, replacement should be planned. The source does not describe exploitation in the wild or give fixed versions, so confirm details with the vendor.

What to do now

1. Inventory applications and third-party components to find any use of Idunno AntiCsrf.
2. Assess which affected assets are reachable from the internet and prioritise those.
3. Apply the vendor's mitigations, or plan migration to a supported version if the product is end-of-life.
4. Stop using the product where no mitigation is available.
5. Review logs and preserve evidence on exposed systems to check for signs of compromise.