EXPLOITED VULNERABILITY ADVISORY: CVE-2026-34486

Summary

CVE-2026-34486 in Apache Tomcat is being actively exploited in the wild. Missing Encryption of Sensitive Data vulnerability in Apache Tomcat due to the fix for CVE-2026-29146 allowing the bypass of the EncryptInterceptor.

This issue affects Apache Tomcat: 11.0.20, 10.1.53, 9.0.116.

Users are recommended to upgrade to version 11.0.21, 10.1.54 or 9.0.117, which fix the issue. CISA requires federal remediation by 2026-08-07; under the CRA, exploitation of an affected product must be reported within 24 hours.

What we know

- **CVE:** CVE-2026-34486
- **Affected:** Apache Tomcat
- **Exploitation:** Actively exploited, added to CISA KEV on 2026-08-04
- **Severity:** CVSS 7.5 High, Network-exploitable, no privileges required, no user interaction (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)
- **Exploitation likelihood (EPSS):** 43%
- **Weakness:** CWE-311

Recommended action

Patch CVE-2026-34486 by 2026-08-07. If you cannot patch immediately, restrict network access to the affected service now (segment it, put it behind a VPN, or take it offline) until you can patch. If you ship an affected product, be ready to file the CRA 24-hour report the moment you find it exploited.

Sources: CISA Known Exploited Vulnerabilities, NIST NVD. Public data; an advisory of active exploitation, not an incident report. Verify applicability to your estate before acting.