EXPLOITED VULNERABILITY ADVISORY: CVE-2026-60004

Summary

CVE-2026-60004 in Gitea Gitea is being actively exploited in the wild. CISA requires federal remediation by 2026-08-28; under the CRA, exploitation of an affected product must be reported within 24 hours.

What we know

- **CVE:** CVE-2026-60004
- **Affected:** Gitea Gitea
- **Exploitation:** Actively exploited, added to CISA KEV on 2026-08-25
- **Weakness:** CWE-94

Recommended action

Patch CVE-2026-60004 by 2026-08-28. Apply mitigations in accordance with vendor instructions, ensuring compliance with CISA's BOD 26-04 Prioritizing Security Updates Based on Risk (see URL in Notes) guidance and CISA's "Forensics Triage Requirements" (see URL in Notes). Follow applicable BOD 26-04 guidance for cloud services or discontinue use of the product if mitigations are unavailable. Stakeholders are responsible for evaluating each asset's internet exposure and ensuring adherence to BOD 26-04 patching guidelines. 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.