

EXPLOITED VULNERABILITY ADVISORY: CVE-2026-72898

Summary

CVE-2026-72898 in Metabase Metabase is being actively exploited in the wild. Metabase allows a remote, unauthenticated attacker to inject arbitrary SQL via the '/reset_password' database endpoint and gain administrator access to the connected Metabase instance. CISA requires federal remediation by 2026-08-14; under the CRA, exploitation of an affected product must be reported within 24 hours.

What we know

- **CVE:** CVE-2026-72898
- **Affected:** Metabase Metabase
- **Exploitation:** Actively exploited, added to CISA KEV on 2026-08-11
- **Severity:** CVSS 10.0 Critical, Network-exploitable, no privileges required, no user interaction (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)
- **Exploitation likelihood (EPSS):** 1%
- **Weakness:** CWE-89

Recommended action

Patch CVE-2026-72898 by 2026-08-14. 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.