



TLP: CLEAR

CALIFORNIA CYBERSECURITY INTEGRATION CENTER



CYBER ADVISORY

Tuesday August 11, 2026

CAL-CSIC-202608-A-003

Critical Vulnerability on Metabase SQL Injection

SQL Injection	Zero-Day Vulnerability	Actively Exploited	Metabase
---------------	------------------------	--------------------	----------

The California Cybersecurity Integration Center (Cal-CSIC) has identified CVE-2026-72898, as a critical SQL injection vulnerability affecting Metabase, a widely employed open-source business intelligence platform.¹ This zero-day vulnerability currently has a Common Vulnerability Scoring System (CVSS) v3.1 base score of 10 and is being exploited in the wild based on a recent CISA Known Exploited Vulnerabilities (KEV) catalog.^{2, 3} Public Proof-of-Concept (PoC) exploit code is currently circulating, and successful exploitation allows an unauthenticated remote attacker full access to compromise backend databases, bypass authentication, and elevate permissions to administrator status.⁴

The Cal-CSIC recommends the following:⁵

1. Immediate Patch Deployment: Prioritize upgrading production and staging self-hosted Metabase deployments to patched releases.
2. Perimeter Hardening: Restrict direct internet access to Metabase management consoles and block or monitor traffic hitting `/api/session/reset_password`.
3. Forensic Audit: Review access logs for the `/api/session/reset_password` endpoint and inspect Metabase user tables for newly created or anomalous administrative accounts created.

The Links below are the Official Documentation on Patch Deployment, Perimeter Hardening and Forensic Audit.

<https://www.metabase.com/blog/security-update>

<https://github.com/metabase/metabase/security/advisories/GHSA-vwf4-m7j8-wcjf>

Affected Components and Versions:

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

TLP: CLEAR

Affected Software	Versions Impacted	Patched Version
Metabase	>= x.58.0, < x.58.24 (or <= x.58.23)	x.58.24
	>= x.59.0, < x.59.21 (or <= x.59.20)	x.59.21
	>= x.60.0, < x.60.17 (or <= x.60.16)	x.60.17
	>= x.61.0, < x.61.11 (or <= x.61.10)	x.61.11
	>= x.62.0, < x.62.9 (or <= x.62.8)	x.62.9
	>= x.63.0, < x.63.5 (or <= x.63.4)	x.63.5

Cal-CSIC services are provided at no cost to assist organizations in strengthening their cybersecurity defenses. If you need assistance or wish to verify this communication, please contact us at (833) REPORT-1, or (916) 636-2997. Visit our website for more details: [California Cybersecurity Integration Center | California Governor's Office of Emergency Services](#)

References:

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

TLP: CLEAR

¹ Metabase; "Security update available for Metabase - Please upgrade now";

<https://www.metabase.com/blog/security-update>; accessed 11 August 2026

² NIST; "CVE-2026-72898 Detail"; <https://nvd.nist.gov/vuln/detail/CVE-2026-72898>; accessed 11 August 2026

³ CISA; "Known Exploited Vulnerabilities Catalog"; <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>; accessed 11 August 2026

⁴ Resecurity; "Metabase Zero-Day Exploited in the Wild: Unauthenticated SQL Injection Leading to Full Admin Access"; <https://www.resecurity.com/blog/article/metabase-zero-day-exploited-in-the-wild-unauthenticated-sql-injection-leading-to-full-admin-access>; accessed 11 August 2026

⁵ Github; "# SQL injection using an unauthenticated endpoint leading to admin access"; <https://github.com/metabase/metabase/security/advisories/GHSA-vwf4-m7j8-wcjf>; accessed 11 August 2026

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

TLP: CLEAR