GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu
Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

12 August 2026

Advisory 186: CVE-2026-72898_Metabase SQL Injection Vulnerability

Release Date: 11th August 2026
Impact: CRITICAL
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that utilize the above products. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-72898 is a critical-severity SQL injection vulnerability in Metabase On-Premises, the open-source business intelligence platform used to visualize data and build dashboards on top of connected databases.
A remote, unauthenticated attacker with HTTP(S) access to a vulnerable Metabase instance can inject arbitrary SQL into the application's own database through the password reset endpoint, gaining administrator access to the instance.

What are the systems affected?

Affected systems include self-hosted Metabase On-Premises instances running one of the vulnerable version ranges listed below. Metabase Cloud has already been remediated by the vendor.

Metabase versions x.63.0 through x.63.4 – (Affected)
Metabase versions x.62.0 through x.62.8 – (Affected)
Metabase versions x.61.0 through x.61.10 – (Affected)

Metabase versions x.60.0 through x.60.16 – (Affected)
Metabase versions x.59.0 through x.59.20 – (Affected)
Metabase versions x.58.0 through x.58.23 – (Affected)
Metabase Cloud – (Remediated by vendor)

Any organisation running self-hosted Metabase for business intelligence or dashboards is at risk, given confirmed active exploitation and the sensitivity of connected database credentials.

What does this mean?

This flaw allows unsanitised input reaching the password reset workflow to be interpreted as SQL by Metabase's own application database. No authentication, credentials, or prior access are required - only network reachability to the Metabase HTTP(S) interface.

Step 1 - Targeting the Password Reset Endpoint
The attacker sends a crafted request to the Metabase password reset API endpoint on an internet-facing or otherwise reachable instance.

Step 2 - SQL Injection
Unsanitised input in the request is passed into a SQL query executed against the Metabase application database, allowing the attacker to inject arbitrary SQL commands.

Step 3 - Administrator Takeover
The injected SQL is used to manipulate the application database directly, allowing the attacker to grant themselves administrator access to the Metabase instance.

Step 4 - Data Access and Exfiltration
With administrator access, the attacker can change the application configuration, **steal stored credentials for every connected database**, and read or export any data reachable through those connections.

Mitigation process

CERTVU recommends the following:

1. **Upgrade Metabase Immediately**

Upgrade self-hosted Metabase instances to the fixed version for your release line: x.63.5+ (from x.63.x), x.62.9+ (from x.62.x), x.61.11+ (from x.61.x), x.60.17+ (from x.60.x), x.59.21+ (from x.59.x), or x.58.24+ (from x.58.x). Given confirmed active exploitation, this should be treated as an emergency and actioned without delay.

Metabase Security Advisory: GHSA-vwf4-m7j8-wcjf

2. **Assume Compromise and Rotate Credentials**

For any internet-facing Metabase instance running an affected version prior to today, treat the instance as potentially compromised: review admin account lists and audit logs for unauthorised

changes, and rotate credentials for all databases connected to Metabase, since stored connection credentials may have already been exposed.

Reference

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://www.cve.org/CVERecord?id=CVE-2026-72898
3. https://github.com/metabase/metabase/security/advisories/GHSA-vwf4-m7j8-wcjf

.