Description

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.

PUBLISHED:	2026-08-10
SCORE:	10 Critical
EPSS:	94.2% High
KEV:	Yes
IMPACT:	n/a
ACTION:	n/a

Analysis

Impact

Metabase contains a remote, unauthenticated SQL injection flaw in the '/reset_password' endpoint that permits an attacker to inject arbitrary SQL statements. Exploiting this defect enables the attacker to bypass authentication entirely and assume full administrator privileges on the connected Metabase instance. The resulting compromise threatens confidentiality, integrity, and availability of all data and administrative controls within the platform.

Affected Systems

All Metabase products are mentioned in the CVE. No specific version information is provided, so any deployment of Metabase is considered potentially vulnerable until the vendor publishes an update.

Risk and Exploitability

The vulnerability carries a CVSS score of 10, an EPSS score of 94%, and is listed in the CISA KEV catalog. The likely attack vector is that attackers can reach the vulnerable endpoint from any network path without authentication, which the description suggests would make exploitation trivial if the database server is exposed online. Based on the description, it is inferred that an attacker can directly access the endpoint without prior authentication and execute arbitrary SQL. Given the severity and high exploitation probability, the risk level is very high and mitigation should be implemented immediately.

Generated by OpenCVE AI on September 6, 2026 at 15:06 UTC.

CVE Mitre Data | CPE Configurations | Affected Packages | OpenCVE Enrichment

Default status is the baseline for the product, each **version** can override it (e.g. patched versions marked unaffected).

Vendor	Product	Default status
Metabase	Metabase	unknown

Versions

Version	Status	Constraints
x.50.0	affected	< x.58.24
x.58.24	unaffected	—
x.59.0	affected	< x.59.21
x.59.21	unaffected	—
x.60.0	affected	< x.60.17
x.60.17	unaffected	—
x.61.0	affected	< x.61.11
x.61.11	unaffected	—
x.62.0	affected	< x.62.9
x.62.9	unaffected	—
x.63.0	affected	< x.63.5
x.63.5	unaffected	—

Remediation

No vendor fix or workaround currently provided.

OpenCVE Recommended Actions

- Update Metabase to the latest version released by the vendor; the patch addresses the SQL injection in the password reset endpoint.
- If an immediate update is not feasible, block or restrict external access to the '/reset_password' endpoint so that only trusted internal users can invoke it.
- Consider disabling the password reset feature entirely for publicly exposed instances until a safe update is applied.
- Verify that the admin account is secured with a strong, unique password and that all default accounts are renamed or removed.

Generated by OpenCVE AI on September 6, 2026 at 15:06 UTC.

Tracking

Sign in to view the affected projects.

Advisories

No advisories yet.

CVSS v4.0 10 Critical | CVSS v3.1 10 Critical | CVSS v3.0 N/A

CVSS v2 N/A | KEV yes | EPSS 0.94217 | SSVC yes

Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
Attack Requirements	None
User Interaction	None
Vulnerable System Confidentiality Impact	High
Vulnerable System Integrity Impact	High
Vulnerable System Availability Impact	High
Subsequent System Confidentiality Impact	High
Subsequent System Integrity Impact	High
Subsequent System Availability Impact	High

References

Link	Providers
https://github.com/met...	CVE NVD
https://raw.githubuserc...	CVE NVD
https://www.cisa.gov/k...	NVD
https://www.cve.org/CV...	CVE NVD
https://www.metabase....	CVE NVD

History

Wed, 12 Aug 2026 15:30:00 +0000

Type	Values Removed	Values Added
Metrics	ssvc {'options': {'Automatable': 'yes', 'Exploitation': 'none', 'Technical Impact': 'total'}, 'version': '2.0.3'}	ssvc {'options': {'Automatable': 'yes', 'Exploitation': 'active', 'Technical Impact': 'total'}, 'version': '2.0.3'}

Wed, 12 Aug 2026 15:15:00 +0000

Type	Values Removed	Values Added
CPEs		cpe:2.3:a:metabase:metabase:*:*:*:*:*:*:*:* cpe:2.3:a:metabase:metabase:*:*:*:*:enterprise:*:*:*

Tue, 11 Aug 2026 21:30:00 +0000

Type	Values Removed	Values Added
Metrics	ssvc {'options': {'Automatable': 'yes', 'Exploitation': 'active', 'Technical Impact': 'total'}, 'version': '2.0.3'}	ssvc {'options': {'Automatable': 'yes', 'Exploitation': 'none', 'Technical Impact': 'total'}, 'version': '2.0.3'}

Tue, 11 Aug 2026 20:30:00 +0000

Type	Values Removed	Values Added
References		• https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-72898
Metrics	ssvc {'options': {'Automatable': 'yes', 'Exploitation': 'none', 'Technical Impact': 'total'}, 'version': '2.0.3'}	ssvc {'options': {'Automatable': 'yes', 'Exploitation': 'active', 'Technical Impact': 'total'}, 'version': '2.0.3'}

Tue, 11 Aug 2026 19:45:00 +0000

Type	Values Removed	Values Added
Metrics		kev {'dateAdded': '2026-08-11T00:00:00+00:00', 'dueDate': '2026-08-14T00:00:00+00:00'}

Tue, 11 Aug 2026 16:30:00 +0000

Type	Values Removed	Values Added
Metrics	ssvc {'options': {'Automatable': 'yes', 'Exploitation': 'active', 'Technical Impact': 'total'}, 'version': '2.0.3'}	ssvc {'options': {'Automatable': 'yes', 'Exploitation': 'none', 'Technical Impact': 'total'}, 'version': '2.0.3'}

Tue, 11 Aug 2026 04:00:00 +0000

Type	Values Removed	Values Added
First Time appeared		Metabase Metabase metabase
Vendors & Products		Metabase Metabase metabase

Mon, 10 Aug 2026 20:30:00 +0000

Type	Values Removed	Values Added
Metrics		ssvc `{'options': {'Automatable': 'yes', 'Exploitation': 'active', 'Technical Impact': 'total'}, 'version': '2.0.3'}`

Mon, 10 Aug 2026 18:15:00 +0000

Type	Values Removed	Values Added
Description		Metabase allows a remote, unauthenticated attacker to inject a '/reset_password' database endpoint and gain administrator a Metabase instance.
Title		Metabase SQL injection via password reset endpoint
Weaknesses		CWE-89
References		• https://github.com/metabase/metabase/security/advisc • https://raw.githubusercontent.com/cisagov/CSAF/devel 26-222-01.json • https://www.cve.org/CVERecord?id=CVE-2026-72898 • https://www.metabase.com/blog/security-update

Metrics		cvssV3_1
		`{'score': 10, 'vector': 'CVSS:3.1/AV:N/AC:L/PR:N`
		cvssV4_0
		`{'score': 10, 'vector': 'CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H`

Subscriptions

Metabase Subscribe

Metabase Subscribe

CVE MITRE

Status: PUBLISHED

Assigner: cisa-cg

Published: 2026-08-10T17:55:54.841Z

Updated: 2026-08-12T14:50:08.735Z

Reserved: 2026-08-10T17:20:39.650Z

Link: CVE-2026-72898

Vulnrichment

Updated: 2026-08-10T20:02:47.250Z

NVD NVD

Status : Analyzed

Published: 2026-08-10T18:18:53.300

Modified: 2026-08-12T15:18:30.347

Link: CVE-2026-72898

Redhat

No data.

OpenCVE Enrichment

Updated: 2026-09-06T15:15:07Z

Weaknesses

- CWE-89
  Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')