

VAULT PANDA Exploits Metabase Vulnerability to Compromise a Telco Operator

Original report published on: August 18, 2026

Executive Summary

On 12 August 2026, CrowdStrike reported that VAULT PANDA (UNC6588) exploited CVE-2026-72898¹, an unauthenticated SQL injection vulnerability in Metabase, against a telecommunications operator and an insurer based in Asia, within one hour after a public exploit template was released². The threat actor (TA) exploited CVE-2026-72898 to gain administrative access to the Metabase business intelligence application, before exploiting CVE-2019-9193 on the underlying operating system (OS), which leverages PostgreSQL's *COPY .. PROGRAM* functionality to execute commands.

Based on the C2 infrastructure, CrowdStrike attributed the activity to VAULT PANDA with high confidence and assessed that the TA would continue to exploit CVE-2026-72898 against Internet-accessible Metabase instances, citing the public availability of a Nuclei template and the lack of authentication or user interaction required for exploitation. As Metabase can access databases containing sensitive information, the potential to chain CVE-2026-72898 with CVE-2019-9193 in PostgreSQL environments to achieve OS-level remote code execution (RCE) makes it a favourable target.

Background

CVE-2026-72898 arose from the interaction of two flaws. Within Metabase's Clojure-based application code, the *merge* function retained a threat actor-supplied *user-id* following failed authentication, while HoneySQL - which Metabase uses to build database queries - interpreted a *:raw* keyword embedded within the supplied *user-id* as an instruction to insert SQL directly into the query rather than treating it as parameterised input, enabling blind SQL injection.

In PostgreSQL environments with the required database privileges, the SQL injection could be used with *COPY .. PROGRAM* functionality to achieve operating system-level remote code execution. Although CVE-2019-9193 has been assigned to this behaviour, both PostgreSQL maintainers and CrowdStrike consider *COPY .. PROGRAM* functionality an intended feature for users with appropriate database privileges.

¹ On 6 August 2026, Metabase disclosed that an actor had exploited CVE-2026-72898 as a zero-day against Metabase Cloud.

² On 12 August 2026, an industry source published a Nuclei template for CVE-2026-72898 that sends three sequential HTTP requests to the `/api/session/reset_password` endpoint to determine whether a Metabase instance is susceptible to SQL injection.

On 12 August 2026, less than an hour after the Nuclei template was publicly released, VAULT PANDA exploited CVE-2026-72898 against a vulnerable Metabase instance and obtained *superuser* access to the backend PostgreSQL database. It subsequently leveraged PostgreSQL's *COPY TO PROGRAM* functionality, associated with CVE-2019-9193, to execute a Base64-encoded script. The script was used to collect system information, test connectivity to 109.104.154[.]238, and attempt DNS- and HTTP-based exfiltration to oob.smartdnslog[.]com.

Detection and Mitigation

IMDA recommends that organisations perform continual testing and validation of existing security controls to ensure detection and prevention against the exploitation of Metabase and PostgreSQL activities identified in this advisory:

- Scan for Indicators of Compromise (Annex A) to detect threat activities in your environment.
- Refer to the MITRE ATT&CK techniques (Annex B) in this advisory to:
 - Create, test and validate detection rules against the threat behaviours.
 - Validate and deny or disable processes, ports and protocols that have no legitimate business need.
- Update all systems, especially internet-facing appliances, to the latest available software or firmware versions.
- Configure PostgreSQL accounts used by Metabase with least privilege and ensure they are not assigned *superuser* or other unnecessary elevated roles, such as *pg_execute_server_program*.
- Restrict publicly accessible services to only those essential for business operations; disable or remove unnecessary services on externally facing servers.
- Enforce internal network access control policies for servers, based on users' roles and requirements (e.g. restrict unnecessary access from DNS servers to other management devices and network infrastructure); where access is necessary, enforce secure authentication mechanisms
- Implement the Snort rule (Annex C), where applicable, to detect network activity associated with exploitation attempts against CVE-2026-72898.
- Implement endpoint detection and response on operating systems, including servers that do not have direct internet exposure and network detection and response to monitor network activity.

Annex A – Indicators of Compromise

This table details the IOCs related to the information provided in this report.

IOC	Description
109.104.154[.]238	VAULT PANDA–controlled C2 server observed in incidents
146.59.252[.]178	VAULT PANDA–controlled IP address observed in incident
oob.smartdnslog[.]com	VAULT PANDA–controlled domain observed in incidents
138.68.51[.]132	IP addresses attempting CVE-2026-72898 exploitation against honeypot infrastructure on 12 August 2026
162.243.242[.]176	
188.253.5[.]80	
27.36.181[.]38	
47.84.122[.]196	
47.251.241[.]219	IP address attempting CVE-2026-72898 exploitation against honeypot infrastructure on 12 and 13 August 2026

Annex B - MITRE ATT&CK Tactics and Techniques

Tactic	Technique	Observable
Resource Development	T1588.005 - Obtain Capabilities: Exploits	The actors and VAULT PANDA likely modified the public Nuclei template to exploit CVE-2026-72898
Initial Access	T1190 - Exploit Public-Facing Application	Across the incidents, actors exploited CVE-2026-72898 against public-facing Metabase instances
Execution	T1059.004 - Command and Scripting Interpreter: Unix Shell	The actors and VAULT PANDA executed Base64-encoded shell scripts via PostgreSQL <i>COPY TO PROGRAM</i> feature
	T1203 - Exploitation for Client Execution	VAULT PANDA chained CVE-2026-72898 with CVE-2019-9193 to achieve RCE
Privilege Escalation	T1068 - Exploitation for Privilege Escalation	CVE-2026-72898 exploitation leads to Metabase <i>superuser</i> database access
Defense Evasion	T1027 - Obfuscated Files or Information	VAULT PANDA Base64-encoded the script used during CVE-2026-72898 exploitation
Discovery	T1082 - System Information Discovery	The script VAULT PANDA deployed collects system information
Collection	T1005 - Data from Local System	VAULT PANDA collected system information and staged it into a file
Command and Control	T1071.001 - Application Layer Protocol: Web Protocols	Actors exploited CVE-2026-72898 via HTTP requests

Annex C – Snort Rule

```
alert tcp any any -> any any (msg: "CrowdStrike Attempted CVE-2026-72898 Metabase SQLi-to-RCE Exploitation Attempt [CSA-260983]"; flow:established,to_server; content:"POST"; http_method; content:"/api/session/reset_password"; http_uri; content:"application/json"; http_header; content:"user-id"; http_client_body; content:"raw"; http_client_body; distance:0; within:50; pcre:"/\"user-id\"\\s*:\\s*\\{\\s*\"raw\"\\s*:/Pi"; classtype:web-application-attack; sid:8002765; rev:20260817;)
```

Reference:

1. [Security update for Metabase](#)
2. [Inside the Metabase SQLi: Exploited in the Wild | Wiz Blog](#)
3. [PostgreSQL - CVE-2019-9193 not a security vulnerability](#)