

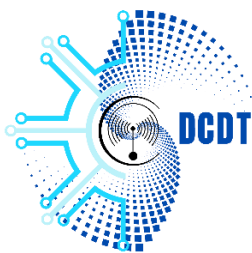
**GOVERNMENT OF THE REPUBLIC
OF VANUATU**

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

10 September 2026

**Advisory 288: AWS Labs Postgres MCP Server OS Command Injection via COPY
TO PROGRAM (CVE-2026-87911).**

Release Date: 9th September 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 deploy the AWS Labs postgres-mcp-server (a component of the official "awslabs/mcp" open-source AWS MCP Servers collection) to connect AI applications or agents to a self-managed PostgreSQL database. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-87911 is a critical OS command injection vulnerability in the SQL validation ("read-only enforcement") component of awslabs.postgres-mcp-server, an official Amazon Web Services (AWS) open-source Model Context Protocol (MCP) server that lets AI applications and agents query and interact with a PostgreSQL database.

What are the systems affected?

The following version(s) are affected:

- awslabs.postgres-mcp-server prior to version 1.1.7 - (Affected)

awslabs.postgres-mcp-server 1.1.7 and later - (Not affected, patched)

What does this mean?

Typical attack flow:

1. **Reach the exposed MCP server in read-only mode**
 - An organisation runs `awslabs.postgres-mcp-server` to let an AI application or agent query a self-managed PostgreSQL database, connecting via the `PG_WIRE_PROTOCOL` method using a database role that holds superuser or `pg_execute_server_program` privileges, and an authenticated user interacts with the server in its intended read-only mode.
2. **Inject a malicious COPY ... TO PROGRAM statement to execute OS commands**
 - An attacker crafts a SQL statement using PostgreSQL's "COPY ... TO PROGRAM" syntax that bypasses the MCP server's read-only enforcement, causing the underlying PostgreSQL server to execute an arbitrary operating system command with the privileges of the database process to achieving remote code execution on the database host itself.

Attack vectors:

- A network-based attack against any deployment of `awslabs.postgres-mcp-server` configured with an over-privileged database role, requiring no attacker authentication but some user interaction with the MCP server.

Successful exploitation may allow attackers to:

- Execute arbitrary operating system commands on the host running the PostgreSQL server behind the MCP integration.
- Use that command execution to access, modify, or exfiltrate any data on the database host, pivot further into the network, or disrupt the availability of the database and any AI application or service depending on it.

Mitigation process

CERTVU recommends the following:

1. Upgrade without delay
 - Update `awslabs.postgres-mcp-server` to version 1.1.7 or later via PyPI.
2. Apply least-privilege database roles to the MCP server's connection
3. Never connect the MCP server as a superuser or cluster master role
4. Layer application-level controls as defence-in-depth

Report any suspected compromise of a self-managed PostgreSQL server exposed via an MCP integration to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. <https://www.cve.org/CVERecord?id=CVE-2026-87911>
2. <https://aws.amazon.com/security/security-bulletins/2026-104-aws/>