مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in pgAdmin 4

Tracking #:432318968

Date:15-05-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities have been identified in pgAdmin 4, culminating in severe risks including authorization bypass, arbitrary SQL execution, server-side request forgery (SSRF), local file disclosure, privilege escalation, and full operating system command execution.

TECHNICAL DETAILS:

Multiple vulnerabilities have been identified in pgAdmin 4, culminating in severe risks including authorization bypass, arbitrary SQL execution, server-side request forgery (SSRF), local file disclosure, privilege escalation, and full operating system command execution.

The most critical issue, tracked as CVE-2026-7813 with a CVSS score of 9.4, allows authenticated attackers to bypass authorization checks and potentially execute arbitrary commands on the host operating system through the Shared Servers feature.

Additional vulnerabilities impact pgAdmin's Export Tool, Maintenance Tool, session handling mechanism, File Manager, and LLM integration functionality.

Vulnerability Details:

- CVE-2026-7813 – Critical (CVSS 9.4)
  Authorization bypass in server mode allowing attackers to access other users' objects and potentially execute OS commands via shared server features.
- CVE-2026-7816 – High
  Export tool command injection via unsafe input in psql \copy, enabling remote OS command execution.
- CVE-2026-7815 – High
  SQL injection in Maintenance Tool fields leading to arbitrary SQL execution and possible OS command execution.
- CVE-2026-7818 – Highl
  Unsafe session file deserialization allowing remote code execution if a malicious session file is placed on the server.
- CVE-2026-7820 – Medium
  Authentication bypass via exposed Flask-Security login endpoint allowing unlimited password guessing.
- CVE-2026-7817 – Medium
  LLM API misconfiguration allowing arbitrary file read and SSRF to internal systems.
- CVE-2026-7819 – High
  File Manager symlink path traversal enabling unauthorized file write outside allowed directories.

Fixed Version

- pgAdmin 4 v9.15

RECOMMENDATIONS:

- Organizations should upgrade pgAdmin to fixed version immediately.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.postgresql.org/about/news/pgadmin-4-v915-released-3295/