مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerabilities in PostgreSQL

Tracking #:432317609

Date:18-08-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities in PostgreSQL that could be exploited to disclose sensitive information, execute arbitrary code during database restoration, and facilitate SQL injection attacks on affected systems.

TECHNICAL DETAILS:

Vulnerability Details:

1. CVE-2025-8713 – Optimizer Statistics Information Disclosure

- **CVSS Score:** 3.1 (Low)
- PostgreSQL optimizer statistics may allow users to read sampled data from views they do not have permission to access. This bypasses row security policies and view access controls, potentially exposing sensitive metadata such as histograms and most-common-values lists.

2. CVE-2025-8714 – Arbitrary Code Execution via pg_dump

- **CVSS Score:** 8.8 (High)
- A malicious superuser of the origin server can craft database objects so that arbitrary code is executed on the client operating system during restoration with psql. This could fully compromise client environments and allow persistent backdoor installation.

3. CVE-2025-8715 – Improper Neutralization of Newlines in pg_dump

- **CVSS Score:** 8.8 (High)
- Improper handling of newline characters in pg_dump enables attackers to inject arbitrary code execution via specially crafted object names. This issue, a regression of CVE-2012-0868, allows both restore-time code execution and SQL injection on the target restore server.

Fixed Versions:

- PostgreSQL 17.6, 16.10, 15.14, 14.19, 13.22, or 18 Beta 3

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the latest security updates released by the vendor.

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/postgresql-176-1610-1514-1419-1322-and-18-beta-3-released-3118/