مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Remote Code Execution Vulnerability in pgAdmin

Tracking #:432318132

Date:15-12-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that a critical Remote Code Execution (RCE) vulnerability has been identified in pgAdmin, the widely used open-source PostgreSQL management tool.

TECHNICAL DETAILS:

A critical Remote Code Execution (RCE) vulnerability has been identified in pgAdmin, the widely used open-source PostgreSQL management tool. Tracked as CVE-2025-13780 with a CVSS v3 score of 9.1, the flaw allows an authenticated attacker to execute arbitrary system commands on the pgAdmin server by abusing a maliciously crafted database restore file. This vulnerability represents a bypass of a previously implemented security fix (CVE-2025-12762) and poses a severe risk to database servers running pgAdmin in server mode.

Vulnerability Details

- **CVE ID:** CVE-2025-13780
- **CVSS v3 Score:** 9.1 (Critical)
- **Vulnerability Type:** Remote Code Execution (RCE)
- **Product:** pgAdmin
- **Deployment Mode Affected:** Server mode
- **Attack Vector:** Malicious database restore (PLAIN-format SQL dump)
- **Affected Versions:** All versions up to and including **pgAdmin 9.10**
- **Fixed Versions**-pgAdmin 9.11 or later

RECOMMENDATIONS:

- Organizations running pgAdmin in server mode should treat this issue as urgent, applying patches or mitigations immediately to prevent exploitation and potential large-scale data and infrastructure compromise.

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://github.com/pgadmin-org/pgadmin4/issues/9368