مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in pgAdmin
Tracking #:432318018
Date:17-11-2025

TLP: WHITE

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed the pgAdmin development team has released a critical security update resolving multiple vulnerabilities, including a critical severity Remote Code Execution (RCE) flaw that could allow attackers to execute arbitrary commands on affected systems.

TECHNICAL DETAILS:

The pgAdmin development team has released a critical security update resolving multiple vulnerabilities affecting all pgAdmin versions up to 9.9. These include a Remote Code Execution (RCE) flaw (CVE-2025-12762, CVSS 9.1), Windows command injection, LDAP injection, and a TLS certificate verification bypass (CVE-2025-12763, CVE-2025-12764, CVE-2025-12765).

Critical Vulnerability Details:
- Critical RCE in PLAIN-Format Restore (CVE-2025-12762)
- Severity: Critical
- CVSS Score: 9.1
- Affected: pgAdmin ≤ 9.9
- Impact: Remote Code Execution during restore operations

Description
- A critical vulnerability exists when pgAdmin is operating in server mode and performing restore operations using PLAIN-format PostgreSQL dump files. Malicious actors can craft specially formed dump files that include system commands, which pgAdmin executes during the restore process.

Other Vulnerabilities Addressed:
- Command injection vulnerability allowing arbitrary command execution on Windows (CVE-2025-12763).
- LDAP authentication flow vulnerable to TLS certificate verification bypass (CVE-2025-12765).
- LDAP injection vulnerability in LDAP authentication flow (CVE-2025-12764).

Fixed Version:
- pgAdmin version 9.10

RECOMMENDATIONS:

- Update pgAdmin to fixed version or the latest available release.

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.pgadmin.org/news/