مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerabilities in pgAdmin

Tracking #:432319173

Date:22-06-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed three critical vulnerabilities have been identified and patched in pgAdmin 4, the widely used graphical administration tool for PostgreSQL databases.

TECHNICAL DETAILS:

Three critical vulnerabilities have been identified and patched in pgAdmin 4, the widely used graphical administration tool for PostgreSQL databases. The vulnerabilities could enable stored Cross-Site Scripting (XSS), authentication bypass, insecure deserialization leading to Remote Code Execution (RCE), and AI Assistant prompt injection resulting in SQL execution.

Vulnerability Details:

1. CVE-2026-12046
    - Severity: Critical
    - CVSS v4 Score: 9.5
    - Unauthenticated pickle deserialization in SQL Editor close / update_connection routes enables remote code execution
2. CVE-2026-12045
    - Severity: Critical
    - CVSS v4 Score: 9.4
    - AI Assistant Prompt Injection/SQL Injection / Read-Only Transaction Bypass
3. CVE-2026-12048
    - Severity: Critical
    - CVSS v4 Score: 9.3
    - Stored XSS via untrusted error and plan-node text rendered through html-react-parser

Fixed Versions:

- pgAdmin version 9.16 or later.

RECOMMENDATIONS:

Immediate Actions:

- Organizations using pgAdmin should upgrade to fixed version immediately, restrict administrative access, secure deployment configurations.

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://nvd.nist.gov/vuln/detail/CVE-2026-12048
- https://nvd.nist.gov/vuln/detail/CVE-2026-12045
- https://nvd.nist.gov/vuln/detail/CVE-2026-12046