مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity COOP Vulnerability in pgAdmin
Tracking #:432317677
Date:08-09-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability tracked as CVE-2025-9636 in pgAdmin that resides in the OAuth authentication flow, which attackers can manipulate to bypass security controls.

TECHNICAL DETAILS:

A newly disclosed Cross-Origin Opener Policy (COOP) vulnerability has been identified in pgAdmin versions 9.7 and earlier. Tracked as CVE-2025-9636, the flaw resides in the OAuth authentication flow, which attackers can manipulate to bypass security controls. Successful exploitation may lead to unauthorized account access, account takeover, data breaches, and privilege escalation.

While exploitation requires low privileges and some user interaction, the impact on confidentiality and integrity is significant. No public proof-of-concept or active exploitation has been observed to date. A patch is available, and organizations are strongly urged to upgrade immediately.

Vulnerability Details
- Vulnerability ID: CVE-2025-9636
- Vulnerability: Cross-Origin Opener Policy (COOP) flaw in OAuth authentication flow.
- Impact: Unauthorized access, privilege escalation, potential account takeover.
- CVSS v3.1 Score: 7.9 (High)
- Affected Product: pgAdmin ≤ 9.7
- Patched Version: pgAdmin 9.8 and later

RECOMMENDATIONS:

- Apply Security Updates: Upgrade pgAdmin version to fixed or newer to remediate the vulnerability.
- Harden Authentication Controls
  - Review and restrict OAuth configurations to trusted providers only.
  - Enforce multi-factor authentication (MFA) for all administrative accounts.
  - Limit pgAdmin access to trusted networks or VPNs.

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/advisories/GHSA-6859-2qxq-ffv2