مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Security Updates - PostgreSQL

Tracking #:432318420

Date:19-02-2026

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that PostgreSQL has released security updates to address multiple vulnerabilities in its products.

TECHNICAL DETAILS:

The PostgreSQL Global Development Group has released security updates for all supported PostgreSQL versions. This release addresses five security vulnerabilities, including memory disclosure and multiple arbitrary code execution issues.

Vulnerability Details
High-Severity Vulnerabilities

- **CVE-2026-2004 – intarray arbitrary code execution**
  Failure to validate input types in the intarray extension's selectivity estimator function may allow an object creator to execute arbitrary code as the operating system user running the database.
- **CVE-2026-2005 – pgcrypto heap buffer overflow**
  A heap buffer overflow in pgcrypto allows a ciphertext provider to execute arbitrary code as the operating system user running the database.
- **CVE-2026-2006 – multibyte character validation arbitrary code execution**
  Missing validation of multibyte character lengths in text manipulation functions allows crafted queries to trigger a buffer overrun, resulting in arbitrary code execution.
- **CVE-2026-2007 – pg_trgm heap buffer overflow**
  A heap buffer overflow in pg_trgm allows a database user to write pattern data into server memory. Potential privilege escalation cannot be ruled out.

Medium-Severity Vulnerability

- **CVE-2026-2003 – oidvector memory disclosure**
  Improper validation of the oidvector type allows a database user to disclose a few bytes of server memory. Although the likelihood of leaking sensitive information is low, this vulnerability could theoretically expose confidential data.

Impact
Successful exploitation of these vulnerabilities may allow an attacker to execute arbitrary code with the database server's privileges and cause crashes or memory corruption. These issues pose a high risk to the confidentiality, integrity, and availability of affected systems,

Fixed Versions:

- PostgreSQL 18.2, 17.8, 16.12, 15.16, and 14.21

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by PostgreSQL.

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-182-178-1612-1516-and-1421-released-3235/