مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates - PostgreSQL

Tracking #:432318991

Date:19-05-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple security vulnerabilities have been addressed in recent releases of PostgreSQL. The update resolves several security flaws ranging from SQL injection and privilege escalation to denial of service, memory disclosure, and arbitrary code execution vulnerabilities.

TECHNICAL DETAILS:

Vulnerability Details

High Severity Vulnerabilities

- **CVE-2026-6473**
  - An integer wraparound issue in multiple PostgreSQL server components may allow out-of-bounds memory writes, potentially causing server crashes or memory corruption.
- **CVE-2026-6475**
  - Improper symlink handling in pg_basebackup and pg_rewind could allow overwriting of arbitrary local files, potentially leading to operating system account compromise.
- **CVE-2026-6476**
  - A SQL injection vulnerability in pg_createsubscriber may allow attackers with subscription creation privileges to execute arbitrary SQL commands with superuser privileges.
- **CVE-2026-6477**
  - Unsafe handling of libpq lo_* functions could allow a malicious PostgreSQL server superuser to overwrite client stack memory, impacting tools such as psql and pg_dump.
- **CVE-2026-6479**
  - An uncontrolled recursion flaw in SSL and GSS negotiation could allow attackers to trigger sustained denial-of-service conditions.
- **CVE-2026-6637**
  - A stack buffer overflow and SQL injection vulnerability in the refint module could allow arbitrary code execution or unauthorized SQL execution.

Medium Severity Vulnerabilities

- **CVE-2026-6472**
  - A missing authorization check in the CREATE TYPE functionality could allow attackers to hijack queries that rely on search_path resolution, potentially leading to execution of arbitrary SQL functions.
- **CVE-2026-6474**
  - A format string vulnerability in the timeofday() function could allow disclosure of portions of server memory through specially crafted timezone inputs.
- **CVE-2026-6478**
  - A timing side-channel vulnerability affecting MD5 password authentication could enable attackers to recover credentials. Systems using scram-sha-256 are not affected.
- **CVE-2026-6575**
  - A buffer over-read vulnerability in pg_restore_attribute_stats() could expose adjacent memory contents during query planning.

Low Severity Vulnerability

- **CVE-2026-6638**
  - A SQL injection issue in logical replication REFRESH PUBLICATION operations could permit execution of arbitrary SQL commands through crafted table names.

Fixed Versions

- PostgreSQL 18.4
- PostgreSQL 17.10
- PostgreSQL 16.14
- PostgreSQL 15.18
- PostgreSQL 14.23

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-184-1710-1614-1518-and-1423-released-3297/