مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

PostgreSQL psql SQL Injection Vulnerability

Tracking #:432316869

Date:14-02-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity SQL injection vulnerability (CVE-2025-1094) has been discovered in PostgreSQL's interactive tool psql.

TECHNICAL DETAILS:

A high-severity SQL injection vulnerability (**CVE-2025-1094**) has been discovered in PostgreSQL's interactive tool psql. This flaw, with a CVSS 3.1 base score of **8.1**, affects all supported versions of PostgreSQL prior to 17.3, 16.7, 15.11, 14.16, and 13.19. The vulnerability allows attackers to achieve arbitrary code execution by exploiting incorrect handling of invalid UTF-8 characters in PostgreSQL's string escaping routines. The vulnerability can be exploited when escaped untrusted input is included as part of a SQL statement executed by the interactive psql tool. Attackers can leverage the incorrect handling of invalid UTF-8 characters to generate a SQL injection.

Successful exploitation of CVE-2025-1094 can lead to:

- Arbitrary code execution (ACE) through the use of meta-commands in psql.
- Execution of unauthorized SQL statements.
- Potential full system compromise if combined with other vulnerabilities.

Affected and Fixed Versions:

Affected Version	Fixed In
17	17.3
16	16.7
15	15.11
14	14.16
13	13.19

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade immediately to the latest patched versions of 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/support/security/CVE-2025-1094/