مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High Severity Vulnerability in PostgreSQL

Tracking #:432316140

Date:13-08-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council observed PostgreSQL released security advisory to address a vulnerability that poses a significant risk of arbitrary SQL execution.

TECHNICAL DETAILS:

A High Severity security vulnerability identified as **CVE-2024-7348** has been disclosed in PostgreSQL, with a **CVSS score of 8.8**. This flaw poses a significant risk of arbitrary SQL execution during pg_dump operations, potentially enabling attackers to exploit the database with elevated privileges.

- **CVE**: **CVE-2024-7348,** CVSS score of 8.8(CNA: PostgreSQL)
- **Vulnerability Type**: Time-of-check Time-of-use (TOCTOU) race condition in pg_dump utility.
- **Impact**: Attackers with permissions to create database objects can exploit the vulnerability to execute malicious SQL code as the superuser running pg_dump, potentially compromising sensitive data and server integrity.
- **Exploit Scenario**: By replacing a relation type (e.g., a table) during pg_dump execution, an attacker can inject harmful SQL functions that leverage the privileges of the pg_dump process.

Affected Versions:

- PostgreSQL 16 before 16.4
- PostgreSQL 15 before 15.8
- PostgreSQL 14 before 14.13
- PostgreSQL 13 before 13.16
- PostgreSQL 12 before 12.20

Fixed versions:

- PostgreSQL 16.4
- PostgreSQL 15.8
- PostgreSQL 14.13
- PostgreSQL 13.16
- PostgreSQL 12.20

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to update PostgreSQL to the latest or fixed version at the earliest.

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-2024-7348//