مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

High-Severity Vulnerability in PostgreSQL

Tracking #:432316523

Date:18-11-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability has been disclosed in PostgreSQL that allows unprivileged users to manipulate environment variables, potentially leading to arbitrary code.

TECHNICAL DETAILS:

A high-severity vulnerability, tracked as **CVE-2024-10979**, has been disclosed in PostgreSQL, a widely used open-source relational database system. This vulnerability, with a CVSS score of 8.8, allows unprivileged users to manipulate environment variables, potentially leading to arbitrary code

Vulnerability Details:

- **Vulnerability ID:** CVE-2024-10979
- **CVSS Score**: 8.8 (High)
- PostgreSQL's PL/Perl extension incorrectly handles environment variables, allowing unprivileged database users to change sensitive environment variables, such as PATH. These environment variables are typically used by applications to configure runtime behavior, such as loading shared libraries or specifying execution paths for commands.
- If exploited, attackers can manipulate the PATH variable, among others, leading to arbitrary code execution or information disclosure. The attacker does not need to have system-level privileges, such as being a superuser or possessing operating system-level access.

Affected Version	Patched Version
17	17.1
16	16.5
15	15.9
14	14.14
13	13.17
12	12.21

RECOMMENDATIONS:

- Upgrade PostgreSQL to one of the patched versions.
- Limit CREATE EXTENSIONS: Restrict the permission to create extensions to only trusted users and administrators. This will prevent unprivileged users from enabling the PL/Perl extension or other extensions that may be vulnerable.
- Implement regular audits of PostgreSQL environments, especially for unusual or unauthorized changes to environment variables.
- Monitor database activity for signs of exploitation, such as unexpected query execution or unauthorized access attempts.

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-2024-10979/