مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates - PHP

Tracking #:432317449

Date:04-07-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed vulnerabilities in PHP that expose applications to SQL injection and denial-of-service (DoS) risks. These issues, tracked as **CVE-2025-1735** and **CVE-2025-6491**, pose significant threats to systems using PostgreSQL and SOAP services.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2025-1735 – SQL Injection & Crashes via PostgreSQL Extension**
  - Affects PHP's pgsql extension.
  - Root cause: Improper error handling in PQescapeStringConn() and PQescapeIdentifier() functions.
  - PHP fails to detect and handle NULL return values, leading to:
    - Potential SQL injection if input is not properly escaped.
    - Null pointer dereference crashes (undefined behavior).
  - PostgreSQL attempts to mitigate encoding issues, but PHP's lack of error propagation leaves applications vulnerable.
- **CVE-2025-6491 – DoS via Oversized XML Namespace in SOAP**
  - Affects PHP's SOAP extension using libxml2.
  - Triggered when a SoapVar is created with a fully qualified XML name >2GB.
  - Causes a NULL pointer dereference due to:
    - Silent failure of xmlNodeSetName() when prefix exceeds INT_MAX.
    - Invalid XML node state leads to segmentation fault during serialization.
  - Easily exploitable using a script like str_repeat("A", 0x7fffffff).

Affected Versions:

- PHP **8.1.x** versions **prior to 8.1.33**
- PHP **8.2.x** versions **prior to 8.2.29**
- PHP **8.3.x** versions **prior to 8.3.23**
- PHP **8.4.x** versions **prior to 8.4.10**

Fixed Versions:

- PHP **8.1.33**
- PHP **8.2.29**
- PHP **8.3.23**
- PHP **8.4.10**

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the necessary patches released by the PHP project 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://github.com/php/php-src/security/advisories/GHSA-hrwm-9436-5mv3