مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in PHP

Tracking #:432316874

Date:17-02-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in PHP that could be exploited to inject malicious code, potentially leading to complete control of affected systems.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2022-31631**
- CVSS Base Score: 9.1 Critical
- A critical vulnerability exists in PHP that can potentially expose websites and applications to SQL injection attacks.
- The flaw resides in the PDO::quote() function when used with SQLite databases, an essential function for escaping user-supplied data before executing database queries. This vulnerability arises from an integer overflow issue that can lead to improper string sanitization, allowing attackers to inject malicious SQL code.
- Successful exploitation could allow attackers to:
    - Inject malicious code
    - Gain control of the database
    - Steal sensitive data
    - Modify database content
    - Gain potential control over the affected system

Affected Versions:

- PHP versions 8.0.x before 8.0.27
- PHP versions 8.1.x before 8.1.15
- PHP versions 8.2.x before 8.2.2

Fixed Versions:

- PHP versions 8.0.27, 8.1.15, or 8.2.2 (or later)

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by PHP.

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://nvd.nist.gov/vuln/detail/CVE-2022-31631