مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

PHP Security Updates

Tracking #:432316556

Date:26-11-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed The PHP development team has released urgent security updates to address multiple critical vulnerabilities in PHP versions.

TECHNICAL DETAILS:

The PHP development team has released urgent security updates to address multiple critical vulnerabilities in PHP versions prior to 8.1.31, 8.2.26, and 8.3.14. These vulnerabilities include remote code execution (RCE) risks, information leakage, and denial-of-service (DoS) attacks, with some vulnerabilities being actively exploitable. The most severe issue, CVE-2024-8932, has been assigned a CVSS score of 9.8, posing significant risks to affected systems. The vulnerabilities affect PHP's LDAP functionality, MySQL integration, stream contexts, and more.

Key Vulnerabilities:

1. **CVE-2024-8932: Out-of-Bounds (OOB) Access in ldap_escape Function**
   - **Severity**: Critical (CVSS 9.8)
   - **Description**: The vulnerability in the ldap_escape function allows for out-of-bounds access on 32-bit systems due to uncontrolled long string inputs. This leads to an integer overflow and could result in arbitrary code execution on the affected system.
2. **CVE-2024-8929: Heap Buffer Over-read Leading to Information Leakage**
   - **Severity**: 5.8 MEDIUM
   - **Description**: This vulnerability enables an attacker to leak partial content from the heap through a buffer over-read, potentially exposing sensitive data. The issue arises when PHP-FPM interacts with a fake MySQL server or through tampered network packets.

Affected Versions: PHP versions prior to 8.1.31, 8.2.26, and 8.3.14
Fixed Versions: PHP 8.1.31,8.2.26,8.3.14

RECOMMENDATIONS:

The UAE Cyber Security Council recommends all users of PHP versions should update to the latest versions.

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-g665-fm4p-vhff