مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Critical Remote Code Execution Vulnerability in Laravel Reverb

Tracking #:432318300

Date:23-01-2026

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical security vulnerability, CVE-2026-23524, has been identified in Laravel Reverb, the real-time WebSocket backend for Laravel applications.

TECHNICAL DETAILS:

A critical security vulnerability, CVE-2026-23524, has been identified in Laravel Reverb, the real-time WebSocket backend for Laravel applications. The flaw allows unauthenticated Remote Code Execution (RCE) under specific deployment conditions.

Vulnerability Details:

- CVE ID: CVE-2026-23524
- CVSS v3.1 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
- CVSS Score: 9.8
- Severity: Critical
- Affected Product: Laravel Reverb
- Affected Versions: Laravel Reverb versions prior to v1.7.0
- Fixed Version: Reverb v1.7.0 and later
- Vulnerability Type: Unsafe PHP Deserialization

RECOMMENDATIONS:

- Immediate Actions: Upgrade Laravel Reverb to fixed version or later across all environments.

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/advisories/GHSA-m27r-m6rx-mhm4