مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Reflected XSS Vulnerabilities in Laravel Framework

Tracking #:432316982

Date:19-03-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that two reflected cross-site scripting (XSS) vulnerabilities identified in the Laravel framework allow attackers to execute arbitrary JavaScript code via maliciously crafted URLs.

TECHNICAL DETAILS:

Security Researchers have identified two reflected cross-site scripting (XSS) vulnerabilities in the Laravel framework, tracked as CVE-2024-13918 and CVE-2024-13919. These vulnerabilities affect Laravel versions 11.9.0 to 11.35.1 and could allow attackers to execute arbitrary JavaScript in a user's browser, leading to potential data theft, session hijacking, or account compromise.

Vulnerability Details

- CVE IDs: CVE-2024-13918 & CVE-2024-13919
- Severity: High
- Affected Product: Laravel Framework
- Impacted Versions: Laravel 11.9.0 – 11.35.1
- Fixed Version: Laravel 11.36.0
- Vulnerability Type: Reflected Cross-Site Scripting (XSS)
- Exploitability: Requires user interaction (clicking on a crafted malicious link)

Technical Summary:

- The vulnerability is caused by improper encoding of URL parameters and request body data in Laravel's debug-mode error page.
- When Laravel's debug mode is enabled, error pages display raw user input without adequate sanitization.
- Attackers can inject malicious JavaScript into request parameters or route parameters, which are then reflected back to the user's browser.
- If a victim clicks on a malicious link, the embedded JavaScript executes in their browser, leading to potential session hijacking, credential theft, or other malicious actions.

RECOMMENDATIONS:

- Upgrade Laravel to fixed version or later to apply fixes for both CVEs.
- Disable Debug Mode (If Upgrade is Not Possible)

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/sbaresearch/advisories/tree/public/2024/SBA-ADV-20241209-01_Laravel_Reflected_XSS_via_Request_Parameter_in_Debug-Mode_Error_Page