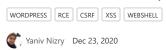
Ξ

Defend your code against SpringShell in two ways: read our blog post with what-to-do advice, and use Checkmarx SCA to test your applications.

RCE Via Site-Offline Wordpress Plugin



Details

Overview

Summary

The site-offline WordPress plugin before version 1.4.4 was vulnerable to Cross-site Request Forgery (CSRF) and Cross-Site Scripting (XSS) attacks.

Product

Site-offline wordpress plugin before version 1.4.4

Impact

Subject to WordPress and server configurations, successful exploitation of the Cross-Site Scripting vulnerability may lead to remote code execution.

Steps To Reproduce

- 1. Setup a WordPress website with the Site Offline plugin installed and activated.
- 2. Admin visits the page



Expected Result:

An alert should be shown on the target WordPress admin panel.

Remediation

Update Site-offline plugin to 1.4.4 or above.

Credit

This issue was discovered and reported by Checkmarx SCA Security Researcher Yaniv Nizry.

Resources

- 1. Changeset
- 2. Site Offline WordPress Plugin