## **Authenticated XSS Vulnerability Discovered in Solidres Hotel Booking Plugin (CVE-2023-1374)**

## 

## **Introduction**

Cross-Site Scripting (XSS) is a security vulnerability that enables attackers to inject malicious code into web pages viewed by other users. These vulnerabilities can be exploited to steal user data, hijack user accounts, and initiate other malicious attacks. In this post, we discuss a POST-based XSS vulnerability discovered in the Solidres – Hotel Booking plugin for WordPress version 0.9.4.

## **Description of the Vulnerability**

The Solidres – Hotel Booking plugin for WordPress version 0.9.4 is susceptible to a POST-based XSS vulnerability within the "add new currency" feature. This vulnerability allows attackers to inject malicious code into the currency\_name parameter of the POST request. The plugin's code does not adequately sanitize the currency\_name parameter, enabling attackers to inject malicious code into the output.

## **Proof of Concept**

Our team has provided a proof of concept using the following curl command to demonstrate the vulnerability:

[**Link to proof of concept**](https://pastebin.com/raw/qxWeQXH7)

## **Impact of the Vulnerability**

Exploiting this vulnerability allows attackers to steal user data, hijack user accounts, and launch other malicious attacks. For example, an attacker can inject a script that steals a user's session cookie, enabling them to take control of the user's account. Additionally, attackers can inject scripts that redirect users to malicious websites, potentially leading to malware downloads onto users' computers.

## **Solution**

To address this vulnerability, the currency\_name parameter of the POST request should be sanitized before being used in the plugin's code. The plugin developers should also implement a Content Security Policy (CSP) to mitigate the impact of any potential XSS attacks. A patch should be released as soon as possible by the plugin developers to fix this vulnerability.

## **Conclusion**

The POST-based XSS vulnerability in the Solidres – Hotel Booking plugin for WordPress version 0.9.4 poses a significant threat to user data, account security, and overall website integrity. The vulnerability exists in the "add new currency" feature of the plugin and can be exploited by injecting a malicious SVG tag into the currency\_name parameter of the POST request. To mitigate this vulnerability, plugin developers should sanitize the currency\_name parameter properly and implement a Content Security Policy (CSP). Users of the plugin should update to the latest version as soon as a patch is released.

## **References**

* [CVE-2023-1374 Record](https://www.cve.org/CVERecord?id=CVE-2023-1374)
* [Wordfence Threat Intelligence](https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/solidres/solidres-094-authenticated-admin-stored-cross-site-scripting)