Back to all zero days

Reflected Cross-Site Scripting (XSS) in Thembay

AFFECTED VENDOR
Thembay

STATUS
Fixed

DATE
Jul 17, 2020

Description Proof of concept (POC) Impact Remediations Timeline

Description

A cross-site scripting (XSS) attack can cause arbitrary code (JavaScript) to run in a user's browser while the browser is connected to a trusted web site. The application targets your users and not the application itself, but it uses your application as the vehicle for the attack. XSS payload was executed when the user loads a malicious link generated using the ajax call back in Greenmart autocomplete search.

Proof of concept: (POC)

The following vulnerability was tested on the Greenmart theme on WordPress with version 5.4.2.

Issue 01: Reflected cross-site scripting.

1. Install the Greenmart theme on WordPress with version 5.4.2.

***Figure-01**: The view-source of the WordPress application, which confirms the theme is Greenmart.*

***Figure-02**: Greenmart search functionality*

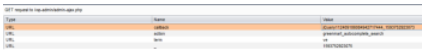

***Figure-03**: The search action related backend ajax call*

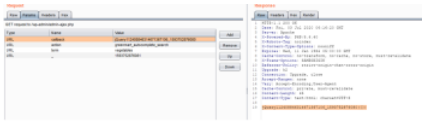

***Figure-04**: The ajax call to "greenmart_autocomplete_search" action and the response from the server*

***Figure-05**: Call-back request parameter with payload and the response from the server.*

2. Click on the following link http://localhost/wordpress/wp-admin/admin-ajax.php?callback=-->%27'><svg/onload=alert(document.cookie)>&action=greenmart_autocomplete_search&term=defaultText&_=1593737670196

***Figure-06**: The call-back parameter is vulnerable to Reflected XSS, and it's getting executed in the user browser context.*

***Figure-07**: Wp-config configuration related to protecting XSS.*

Impact

When the user input from a URL or POST data is reflected on the page without being stored, thus allowing the attacker to inject malicious content. This means that an attacker has to send a crafted malicious URL or post form to the victim to insert the payload.

Remediations

Download and apply the relevant patches from the vendor.

Affected Vendor
Thembay

Bug Name
Reflected Cross-Site Scripting (XSS)

CVE Number
CVE-2020-16140

CWE ID
CWE - 787

CSW ID
2020-CSW-07-1045

CVSSv3 Score
7.9

Affected Version
5.4.2

Severity
High

Affected Product
Greenmart version 2.4.2.

July 18, 2020: Vendor Released Fixed

July 29, 2020: CVE Assigned

Discovered by

Cyber Security Works Pvt. Ltd.