‹ Back to all zero days

Stored Cross-Site Scripting (XSS) in WordPress Plugin (ZOHO CRM Lead Magnet Version 1.7.2.4)

AFFECTED VENDOR	STATUS	DATE
Wordpress 5.8	Fixed	Sep 1, 2021

Medium Severity

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 website. The attack targets your application's users and not the application itself while using your application as the attack's vehicle. The XSS payload executes whenever the user changes the form values or deletes a created form in Zoho CRM Lead Magnet Version 1.7.2.4.

Proof of concept: (POC)

The following vulnerability was detected in Zoho CRM Lead Magnet Version 1.7.2.4

Issue: Stored Cross-Site Scripting.

Steps to reproduce:

1. Log in to the WordPress application.

Note: A virtual host (wptest.com) was used to test the application locally.

2. Install the Zoho CRM Lead Magnet Plugin.

Figure 01: *Zoho CRM Lead Magnet Version 1.7.2.4*

3. Configure the Client ID and Secret Key.

4. Click the 'Create New Form' button, fill the values, and then click the 'Next' button.

Figure 02: *New form in Zoho CRM Plugin*

5. Encode the payload <img src=x onerror=alert(document.cookie)> with a hexadecimal HTML encoder.

Figure 03: *Encoding the Payload*

6. Enter the encoded payload in the 'Form Name' field (formvalue parameter) to update the form. Then, click the arrow button near the 'Create a New Form' heading to go back to the previous page.

Figure 04: *Entering Encoded Xss Payload In The 'form Name' Field*

7. Click on the pencil icon to edit the created form.

Affected Vendor	Wordpress 5.8
Bug Name	Stored Cross-Site Scripting
CVE Number	CVE-2021-33849
CWE ID	CWE-79
CSW ID	2021-CSW-08-1050
CVSSv3 Score	6.1
Affected Version	Version 1.7.2.4
Severity	Medium
Affected Product	Zoho Lead Magnet Plugin

Figure 05: *Click on the Pencil Icon to Edit the Form*

8. Change any form value, such as 'Company' or the 'Last Name'.

Figure 06: *Modifying Form Fields*

Figure 07: *Injected XSS Payload Executed Displaying An Alert Box With Contents of the User's Cookies*

9. The XSS payload is also executed when the user tries to delete the form.

Figure 08: *XSS Payload Executed When the User Tries To Delete the Form*

Impact

With Cross-Site Scripting, an attacker can control a script executed in the victim's browser and then fully compromise that user. An XSS vulnerability enables attacks that are self-contained within the application. This means that an attacker does not need to find an external means of inducing the victim to make a request containing their exploit. Rather, the attacker can insert the exploit into the application and simply wait for users to encounter it.

A Cross-Site Scripting attack results in the following:

● Cookie theft

● Disclosure of end-user files

● Installation of Trojan horse programs

● Redirection of user to some other page or site

Remediations

To fix this vulnerability, follow these steps:

- Perform context-sensitive encoding of untrusted input before it is echoed back to a browser by using the encoding library.
- Implement input validation for special characters on all variables reflected to the browser and stored in the database.
- Implement client-side validation.

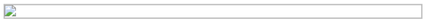

__Figure 09:__ Default Cross-Site Scripting Mitigation Setting in the wp.config File Prevents Cross-site Scripting Attacks

Timeline

- **Aug 26, 2021:** Discovered in Zoho CRM Lead Magnet Version 1.7.2.4.
- **Sep 1, 2021:** Reported to WordPress Team
- **Sep 2, 2021:** Vendor Acknowledged
- **Sep 2, 2021:** Vendor blocked the plugin
- **Sep 6, 2021:** Zoho fixed the issue
- **Sep 7, 2021:** Vendor reopened the plugin for download.
- **Sep 7, 2021:** CVE Assigned.

Discovered by

Cyber Security Works Pvt. Ltd.

Advisory

Security Advisory Published by WordPress.

Talk to CSW's team of experts to secure your landscape.

Schedule free consultation

Cyber Security Works helps reduce security debt and inherent vulnerabilities in an organization's infrastructure and code. We work with large public, private, and start-up companies and help them prioritize their vulnerabilities.

Resources

Ransomware
Cyber Risk Series
Blogs
Patch Watch
Data Sheets
White Papers
Zero Days
Glossary
Events
CISA-KEV

Partner

Become a Partner

Quick Links

About Us
Contact Us
Careers
Services
Media Coverage
Cybersecurity month
Predictions for 2022
Cybersecurity for govt
Hackathon

Sitemap Privacy Policy Customer Agreements