

[← Back to all zero days](#)

Stored Cross-Site Scripting in WordPress Customize Login Image

AFFECTED
VENDOR

WordPress

STATUS

Fixed

DATE

Dec 2, 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 opens the login page of the WordPress application.

Proof of concept: (POC)

The following vulnerability was discovered in Customize Login Image version 3.4.

Issue: Stored Cross-Site Scripting

1. Login to the WordPress application.

Note: A virtual host (wptest.com) is used for testing the application locally.

2. Install the Customize Login Image Plugin.
3. Go to the 'Settings' menu and click on the 'Customize Login Image' drop list.



Affected Vendor

WordPress

Bug Name

Stored Cross-Site Scripting

CVE Number

[CVE-2021-33851](#)

CWE ID

CWE-79

CSW ID

2021-CSW-11-1052

CVSSv3 Score

6.1

Affected Version

Version 3.4

Severity

Medium

Affected Product

Customize Login Image



Figure 01: Customize Login Image Plugin

4. Enter the payload - `<script>alert(document.cookie)</script>` in the 'Custom Logo Link' field (cli_logo_url parameter).



Figure 02: Entering encoded XSS payload in the 'Custom Logo Link' field

5. Click on the 'Save Changes' button
6. Go to the WordPress login page at /wp-login.php .



Figure 03: Injected XSS payload is executed and displays an alert box containing the user's cookies.

Impact

An attacker can perform the following:

- Inject malicious code into the vulnerable variable and exploit the application through the Cross-Site Scripting vulnerability.
- Modify the code and get the session information of other users.
- Compromise the user machine.

Remediations

Cookies.
This site uses cookies to give you a better experience. By using our site you agree to the use of cookies. See our [cookie policy](#) for more details.

I Accept

at before echoing back to a
application.

all the variables are

e generated by the

- Encode dynamic output elements and filter specific characters in dynamic elements.



Figure 04: The default Cross-Site Scripting mitigation setting in wp.config file to prevent XSS attacks

Timeline

Nov 30, 2021: Discovered in 'Customize Login Image version 3.4' Product

Dec 2, 2021: Reported to WordPress team

Dec 7, 2021: Vendor **fixed** the issue

Dec 7, 2021: Vendor reopened the plugin for download

Dec 10, 2021: CVE assigned

Additional Notes

[Security Advisory Published by WordPress](#)

Discovered by

Cyber Security Works Pvt. Ltd.

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.



[Sitemap](#) [Privacy Policy](#) [Customer Agreements](#)
© 2022 - Cyber Security Works

Resources

[Ransomware](#)
[Cyber Risk Series](#)
[Blogs](#)
[Patch Watch](#)
[Data Sheets](#)
[White Papers](#)
[Zero Days](#)
[Glossary](#)
[Events](#)
[CISA-KEY](#)

Partner

[Become a Partner](#)

Quick Links

[About Us](#)
[Contact Us](#)
[Careers](#)
[Services](#)
[Media Coverage](#)
[Cybersecurity month](#)
[Predictions for 2022](#)
[Cybersecurity for govt](#)
[Hackathon](#)