

[← Back to all zero days](#)

Stored cross site scripting (XSS) in WordPress Microsoft Clarity Plugin

AFFECTED
VENDOR
Microsoft

STATUS
Fixed

DATE
Oct 18, 2021



Medium Severity

Description

Proof of concept (POC)

Impact

Remediations

Timeline

Description

A Cross-Site Scripting vulnerability in Microsoft Clarity version 0.3 can cause arbitrary code to run in a user's browser while the browser is connected to a trusted website. The XSS payload executes whenever the user changes the clarity configuration in Microsoft Clarity version 0.3 stored on the configuring project ID page.

Proof of concept: (POC)

The following vulnerability was detected in WordPress Microsoft Clarity Plugin version 0.3.

1. Log in to the WordPress application.
2. Install Microsoft Clarity plugin to your WordPress application.



Affected Vendor

Microsoft

Bug Name

Cross-Site Scripting

CVE Number

[CVE-2021-33850](#)

CWE ID

CWE-79

CSW ID

2020-CSW-10-1050

CVSSv3 Score

4.9

Affected Version

version 0.3

Severity

Medium

Affected Product

Microsoft Clarity version 0.3



Figure 1: Microsoft Clarity Plugin Installation

3. Click on Settings, and the Clarity Setting page appears.



Figure 2: Microsoft Clarity Settings Page

4. In the Clarity Settings page, enter the payload in the 'project ID' section (clarity_project_id parameter).



Figure 3: Entering Encoded Xss Payload in the Project ID section

5. Injected XSS payload gets executed whenever the user changes the clarity configuration page.



Figure 4: Injected XSS Payload Executed and Displays an Alert Box

Impact

An attacker can control a script executed in the victim's browser and fully compromise the targeted user. In addition, an XSS vulnerability enables attacks that are contained within the application itself. There is no need to find an external way of inducing the victim to make a request containing their exploit. Instead, the attacker places the exploit inside the application itself and simply waits for users to encounter it, thus, resulting in the following --

- Stealing cookies,
- End-user files disclosure,
- Installation of Trojan horse programs.

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

It before it is echoed back

2. Implement input validation for special characters on all the variables reflected in the browser and stored in the database.
3. Implement client-side validation.



Figure 5: Cross-Site Scripting Mitigation Setting in the wp.config File Prevents Cross-site Scripting Attacks

Timeline

- 17 October 2021:** Discovered in Microsoft Clarity version 0.3
- 20 October 2021:** Reported to WordPress Team.
- 20 October 2021:** WordPress acknowledged.
- 25 October 2021:** Microsoft Clarity Plugin fixed the issue.
- 07 November 2021:** CSW Assigned the CVE Identifier [CVE-2021-33850]

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](#)