

[← Back to all zero days](#)

Multiple Cross-Site Scripting (XSS) in Openfire Product

AFFECTED

VENDOR

Ignite

Realtime

Openfire

STATUS

Fixed

DATE

Feb 5, 2020



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 web site. The application targets your application's users and not the application itself, but it uses your application as the vehicle for the attack. XSS payload is executed whenever the user views the crafted POST request with XSS Payload in Openfire 4.5.0 Product.

Proof of concept: (POC)

The following vulnerability was tested on Openfire version 4.5.0 Product.

Issue 01: Reflected cross-site scripting

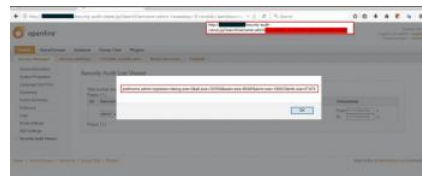


Figure 01: Injected XSS payload "+accesskey='X'+onclick='alert(document.cookie);" gets reflected in the browser response.

Issue 02: Reflected cross-site scripting

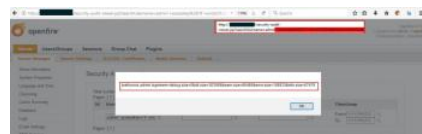


Figure 02: Injected XSS payload "+accesskey='X'+onclick='alert(document.cookie);" gets reflected in the browser response.

Affected Vendor

Ignite Realtime Openfire

Bug Name

Multiple Cross-Site Scripting (XSS)

CVE Number

[CVE-2020-24601](#)

CWE ID

CWE - 79

CSW ID

2020-CSW-01-1039

CVSSv3 Score

6.1

Affected Version

4.5.0

Severity

Medium

Affected Product

Openfire



Impact

- Stealing cookies
- End-user files disclosure.
- Redirection of the user to some other page or site.

Remediations

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

Timeline

Feb 04, 2020: Vulnerability Discovered by CSW Security Researcher.

Feb 05, 2020: Vulnerability Reported to Vendor

Feb 06, 2020: Vendor responded with bug tracker Links

Feb 13, 2020: Follow up with vendor for fix release

Mar 01, 2020: Follow up with Vendor for fix release

Mar 06, 2020: Vendor responded with released fix

Aug 20, 2020: Request for CVE

Aug 24, 2020: CVE Assigned

Sep 01, 2020: Vendor Updated CVE in the bug tracker and Request for an update in CVE

Sep 02, 2020: CVE Published in NVD

Discovered by

Cyber Security Works Pvt. Ltd.

Advisory

[Security Advisory Published by Openfire](#)

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-KEV](#)

Partner

[Become a Partner](#)

Quick Links

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