< Back to all zero days

Multiple Cross-Site Scripting (XSS) in Openfire Product

AFFECTED VENDOR	STATUS	DATE
Ignite Realtime Openfire	Fixed	Feb 4, 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 (POST Request)

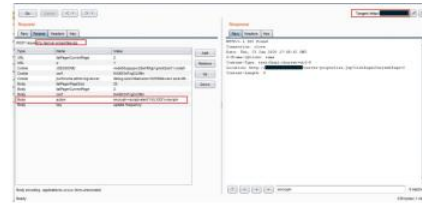**Figure 01**: System Properties page

Figure 02: Request to the server with malicious payload > in the parameter 'action.'
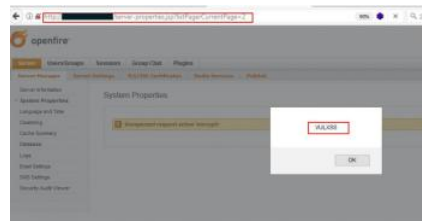

Figure 03: Malicious JavaScript payload is executed on the victim's browser

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

Sidebar

Affected Vendor
Ignite Realtime Openfire

Bug Name
Multiple Cross-Site Scripting (XSS)

CVE Number
CVE-2020-24602

CWE ID
CWE - 79

CSW ID
2020-CSW-01-1040

CVSSv3 Score
6.1

Affected Version
4.5.0

Severity
Medium

Affected Product
Openfire

† Request for an update in

Additional Notes

Jan 28, 2020 – Discovered in Openfire version 4.5.0.

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