< Back to all zero days

Multiple Cross Site Scripting (XSS) in Openfire Product

AFFECTED VENDOR	STATUS	DATE
Ignite Realtime Openfire	Fixed	Feb 5, 2020

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: Stored cross-site scripting

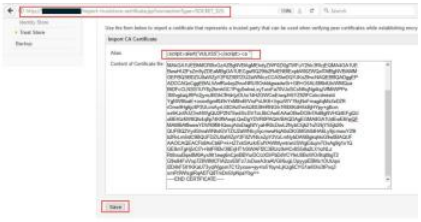

Figure 01: *Import CA Certificate page with malicious payload "> in alias parameter*

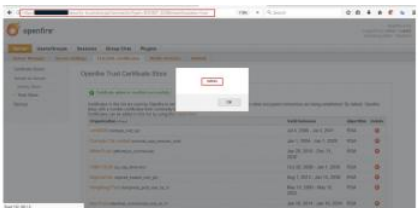

Figure 02: *Malicious JavaScript payload is executed on the victim's browser every time this page is visited*

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 the browser and storing 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

Affected Vendor
Ignite Realtime Openfire

Bug Name
Multiple Cross Site Scripting (XSS)

CVE Number
CVE-2020-24604

CWE ID
CWE - 79

CSW ID
2020-CSW-01-1041

CVSSv3 Score
6.1

Affected Version
4.5.0

Severity
Medium

Affected Product
Openfire

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