

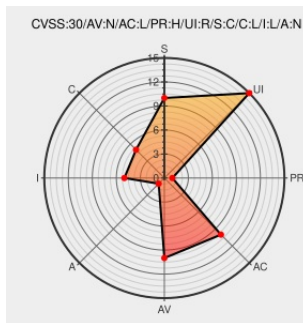


CVE-2017-15911

Published on: 10/26/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:34 PM UTC

CVE-2017-15911

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Openfire](#) from [Igniterealtime](#) contain the following vulnerability:

The Admin Console in Ignite Realtime Openfire Server before 4.1.7 allows arbitrary client-side JavaScript code execution on victims who click a crafted `setup/setup-host-settings.jsp?domain=` link, aka XSS. Session ID and data theft may follow as well as the possibility of bypassing CSRF protections, injection of iframes to establish communication channels, etc. The vulnerability is present after login into the application.

CVE-2017-15911 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **4.8 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	HIGH	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	LOW	NONE

CVSS2 Score: **3.5 - LOW**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Become P3NTESTER: XSS Vulnerability in Openfire - 4.1.6 - [CVE-2017-15911]	Issue Tracking Third Party Advisory	MISC becomepentester.blogspot.ae/2017/10/Cross-Site-

becomepentester.blogspot.ae
text/html

[Scripting-Openfire-4.1.6-CVE-2017-15911.html](#)

[OF-1417] CVE-2017-15911 XSS with domain in setup-host-settings.jsp - IgniteRealtime JIRA

[Issue Tracking](#)
[Vendor Advisory](#)
issues.igniterealtime.org
text/html

[MISC issues.igniterealtime.org/browse/OF-1417](https://issues.igniterealtime.org/browse/OF-1417)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Igniterealtime	Openfire	All	All	All	All
cpe:2.3:a:igniterealtime:openfire:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)