



CVE-2019-15488

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2019-15488
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-08-23 13:15:00 UTC
Updated	2019-08-26 21:02:00 UTC
Description	Ignite Realtime Openfire before 4.4.1 has reflected XSS via an LDAP setup test.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Igniterealtime	Openfire	All	All	All	All
Application	Igniterealtime	Openfire	All	All	All	All

References

Reference	Source	Link
OF-1192: Fixes Reflected XSS in LDAP Setup test by guusdk · Pull Request #1441 · igniterealtime/Openfire · GitHub	MISC	github.cc
Comparing cd0a573...5e5d9e5 · igniterealtime/Openfire · GitHub	MISC	github.cc
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[981663](#) Java (maven) Security Update for org.igniterealtime.openfire:xmppserver (GHSA-5qfv-rr79-chx5)

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](#)