



CVE-2015-7707

Published on: 10/05/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:12 PM UTC

CVE-2015-7707

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

Ignite Realtime Openfire 3.10.2 allows remote authenticated users to gain administrator access via the isadmin parameter to user-edit-form.jsp.

CVE-2015-7707 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **6.5 - MEDIUM**

Access Vector

NETWORK

Access Complexity

LOW

Authentication

SINGLE

Confidentiality Impact

PARTIAL

Integrity Impact

PARTIAL

Availability Impact

PARTIAL

CVE References

Description

Tags

Link

Openfire 3.10.2 - Privilege Escalation - JSP webapps Exploit

[Exploit](#)
www.exploit-db.com
[Proof of Concept](#)
[text/html](#)

[EXPLOIT-DB 38190](#)

Openfire 3.10.2 Privilege Escalation ~ Packet Storm

[Exploit](#)
packetstormsecurity.com
[text/html](#)

[MISC](#)
packetstormsecurity.com/files/133559/Openfire-3.10.2-Privilege-Escalation.html

[OF-941] CVE-2015-7707 Admin Console Privilege Escalation Vulnerability - IgniteRealtime JIRA

igniterealtime.org
[text/html](#)

[MISC igniterealtime.org/issues/browse/OF-941](#)

Openfire: Multiple vulnerabilities (GLSA 201612-50) — Gentoo security

security.gentoo.org
[text/html](#)

[GENTOO GLSA-201612-50](#)

hyp3rlinx.altevista.org
[text/plain](#)

[MISC hyp3rlinx.altevista.org/advisories/AS-OPENFIRE-PRIV-ESCALATION.txt](#)

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	3.10.2	All	All	All
Application	Igniterealtime	Openfire	3.10.2	All	All	All
cpe:2.3:a:igniterealtime:openfire:3.10.2:*:*:*:*:*:						
cpe:2.3:a:igniterealtime:openfire:3.10.2:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)