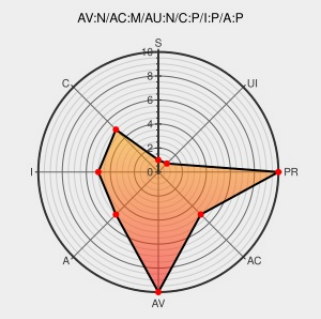
CVE-2015-6973

Published on: 09/16/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:17 PM UTC

CVE-2015-6973

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Openfire from Igniterealtime contain the following vulnerability:

Multiple cross-site request forgery (CSRF) vulnerabilities in Ignite Realtime Openfire 3.10.2 allow remote attackers to hijack the authentication of administrators for requests that (1) change a password via a crafted request to user-password.jsp, (2) add users via a crafted request to user-create.jsp, (3) edit server settings or (4) disable SSL on the server via a crafted request to server-props.jsp, or (5) add clients via a crafted request to plugins/clientcontrol/permitted-clients.jsp.

CVE-2015-6973 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 6.8 - MEDIUM

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

CVE References

Description	Tags	Link
Openfire 3.10.2 - CSRF Vulnerabilities	Exploit, www.exploit-db.com, Proof of Concept, text/html	EXPLOIT-DB 38192
SecurityFocus	web.archive.org, text/html, Inactive Link, Not Archived	BUGTRAQ 20150915 Openfire 3.10.2 CSRF Vulnerabilities
Openfire 3.10.2 Cross Site Request Forgery ≈ Packet Storm	packetstormsecurity.com, text/html	MISC packetstormsecurity.com/files/133554/Openfire-3.10.2-Cross-Site-Request-Forgery.html

Openfire: Multiple vulnerabilities (GLSA 201612-50) — Gentoo security	security.gentoo.org text/html	GENTOO GLSA-201612-50
	hyp3rlinx.altervista.org text/plain	MISC hyp3rlinx.altervista.org/advisories/AS-OPENFIRE-CSRF.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→