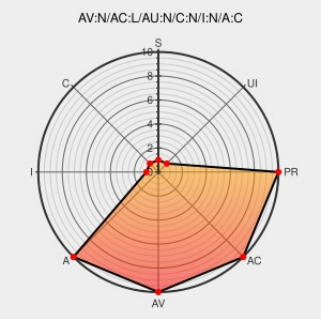
CVE-2014-2741

Published on: 04/10/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:58 PM UTC

CVE-2014-2741

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



Certain versions of Openfire from Igniterealtime contain the following vulnerability:

nio/XMLLightweightParser.java in Ignite Realtime Openfire before 3.9.2 does not properly restrict the processing of compressed XML elements, which allows remote attackers to cause a denial of service (resource consumption) via a crafted XMPP stream, aka an "xmppbomb" attack.

CVE-2014-2741 has been assigned by security@debian.org to track the vulnerability

CVSS2 Score: 7.8 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	COMPLETE

CVE References

Description	Tags	Link
oss-security - Re: Possible CVE Request: Uncontrolled Resource Consumption with XMPP-Layer Compression	openwall.com text/html	MLIST [oss-security] 20140407 Re: Possible CVE Request: Uncontrolled Resource Consumption with XMPP-Layer Compression
Ignite Realtime: Security Issue: Uncontrolled Resource...	community.igniterealtime.org text/html	CONFIRM community.igniterealtime.org/thread/52317
Uncontrolled Resource Consumption with XMPP-Layer Compression – The XMPP Standards Foundation	web.archive.org text/html Inactive Link Not Archived	MISC xmpp.org/resources/security-notices/uncontrolled-resource-consumption-with-highly-compressed-xmpp-stanzas/
oss-security - Re: (Openfire M-Link Metronome Prosody Tigase) Possible CVE Request: Uncontrolled Resource Consumption with XMPP-Layer Compression	openwall.com text/html	MLIST [oss-security] 20140408 Re: (Openfire M-Link Metronome Prosody Tigase) Possible CVE Request: Uncontrolled Resource Consumption with XMPP-Layer Compression

Vulnerability Note VU#495476 - Openfire contains an uncontrolled resource consumption vulnerability	US Government Resource www.kb.cert.org text/html	CERT-VN VU#495476
FishEye: changeset 3aec383e07ee893b77396fe946766bbd3758af77	web.archive.org text/html Inactive Link Not Archived	CONFIRM fisheye.igniterealtime.org/changelog/openfiregit?cs=3aec383e07ee893b77396fe946766bbd3758af77

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→