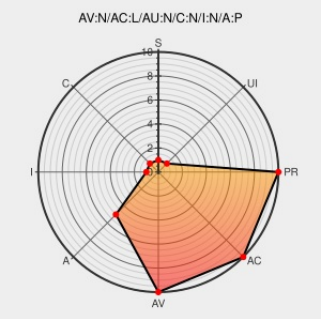
CVE-2004-1378

Published on: 09/21/2004 04:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:10 PM UTC

CVE-2004-1378

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



Certain versions of Jabberd from Jabberstudio contain the following vulnerability:

The expat XML parser code, as used in the open source Jabber (jabberd) 1.4.3 and earlier, jadc2s 0.9.0 and earlier, and possibly other packages, allows remote attackers to cause a denial of service (application crash) via a malformed packet to a socket that accepts XML connections.

CVE-2004-1378 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
Secunia - Advisories - jabberd / jadc2s XML Parsing Denial of Service Vulnerability	web.archive.org, text/html	SECUNIA 12636
SecurityTracker.com Archives - jabberd XML Parsing Bug Lets Remote Users Crash the Service	securitytracker.com, text/html	SECTRACK 1011383
Index of /jabberd14	Patch, web.archive.org, text/html, Inactive Link, Not Archived	CONFIRM devel.amessage.info/jabberd14/
Gentoo Linux Documentation -- jabberd 1.x: Denial of Service vulnerability	Patch, www.gentoo.org, text/html	GENTOO GLSA-200409-31

Jabber Studio JabberD Remote Denial Of Service Vulnerability	Patch cve.report (archive) text/html	BID 11231
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF jadc2s-xml-dos(17467)
SecurityTracker.com Archives - jadc2s XML Parsing Bug Lets Remote Users Crash the Service	securitytracker.com text/html	SECTRACK 1011384
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 10257
[jabberd] Jabberd 1.4 critical bug	web.archive.org text/html Inactive Link Not Archived	MLIST [jabberd] 20040919 Jabberd 1.4 critical bug
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF jabberd-xml-dos(17466)
VuXML: jabberd -- denial-of-service vulnerability	www.vuxml.org text/html	CONFIRM www.vuxml.org/freebsd/2e25d38b-54d1-11d9-b612-000c6e8f12ef.html
'Possible DoS attack against jabberd 1.4.3 and jadc2s 0.9.0' - MARC	marc.info text/html	BUGTRAQ 20040920 Possible DoS attack against jabberd 1.4.3 and jadc2s 0.9.0

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Jabberstudio	Jabberd	1.4	All	All	All
Application	Jabberstudio	Jabberd	1.4.1	All	All	All
Application	Jabberstudio	Jabberd	1.4.2	All	All	All
Application	Jabberstudio	Jabberd	1.4.2a	All	All	All
Application	Jabberstudio	Jabberd	1.4.3	All	All	All
Application	Jabberstudio	Jabberd	1.4	All	All	All
Application	Jabberstudio	Jabberd	1.4.1	All	All	All
Application	Jabberstudio	Jabberd	1.4.2	All	All	All
Application	Jabberstudio	Jabberd	1.4.2a	All	All	All
Application	Jabberstudio	Jabberd	1.4.3	All	All	All
Application	Jabberstudio	Jadc2s	0.6	All	All	All
Application	Jabberstudio	Jadc2s	0.7	All	All	All
Application	Jabberstudio	Jadc2s	0.8	All	All	All

Application	Jabberstudio	Jadc2s	0.9	All	All	All
Application	Jabberstudio	Jadc2s	0.6	All	All	All
Application	Jabberstudio	Jadc2s	0.7	All	All	All
Application	Jabberstudio	Jadc2s	0.8	All	All	All
Application	Jabberstudio	Jadc2s	0.9	All	All	All

cpe:2.3:a:jabberstudio:jabberd:1.4:*:*:*:*:*:*:*:

cpe:2.3:a:jabberstudio:jabberd:1.4.1:*:*:*:*:*:*:*:

cpe:2.3:a:jabberstudio:jabberd:1.4.2:*:*:*:*:*:*:*:

cpe:2.3:a:jabberstudio:jabberd:1.4.2a:*:*:*:*:*:*:*:

cpe:2.3:a:jabberstudio:jabberd:1.4.3:*:*:*:*:*:*:*:

cpe:2.3:a:jabberstudio:jabberd:1.4:*:*:*:*:*:*:*:

cpe:2.3:a:jabberstudio:jabberd:1.4.1:*:*:*:*:*:*:*:

cpe:2.3:a:jabberstudio:jabberd:1.4.2:*:*:*:*:*:*:*:

cpe:2.3:a:jabberstudio:jabberd:1.4.2a:*:*:*:*:*:*:*:

cpe:2.3:a:jabberstudio:jabberd:1.4.3:*:*:*:*:*:*:*:

cpe:2.3:a:jabberstudio:jadc2s:0.6:*:*:*:*:*:*:*:

cpe:2.3:a:jabberstudio:jadc2s:0.7:*:*:*:*:*:*:*:

cpe:2.3:a:jabberstudio:jadc2s:0.8:*:*:*:*:*:*:*:

cpe:2.3:a:jabberstudio:jadc2s:0.9:*:*:*:*:*:*:*:

cpe:2.3:a:jabberstudio:jadc2s:0.6:*:*:*:*:*:*:*:

cpe:2.3:a:jabberstudio:jadc2s:0.7:*:*:*:*:*:*:*:

cpe:2.3:a:jabberstudio:jadc2s:0.8:*:*:*:*:*:*:*:

cpe:2.3:a:jabberstudio:jadc2s:0.9:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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