



CVE-2010-0305

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2010-0305
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-02-03 19:30:00 UTC
Updated	2026-04-29 01:13:23 UTC
Description	ejabberd_c2s.erl in ejabberd before 2.1.3 allows remote attackers to cause a denial of service (daemon crash) via a large n

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

AV:N/AC:L/Au:N/C:N/I:N/A:P

Problem Types: CWE-20 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

AV:N/AC:L/Au:N/C:N/I:N/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Process-one	Ejabberd	0.9	All	All	All

Application	Process-one	Ejabberd	0.9.1	All	All	All
Application	Process-one	Ejabberd	0.9.8	All	All	All
Application	Process-one	Ejabberd	1.0.0	All	All	All
Application	Process-one	Ejabberd	1.1.0	All	All	All
Application	Process-one	Ejabberd	1.1.1	All	All	All
Application	Process-one	Ejabberd	1.1.1.0	All	All	All
Application	Process-one	Ejabberd	1.1.1.1	All	All	All
Application	Process-one	Ejabberd	1.1.14	All	All	All
Application	Process-one	Ejabberd	1.1.2	All	All	All
Application	Process-one	Ejabberd	1.1.3	All	All	All
Application	Process-one	Ejabberd	2.0.0	All	All	All
Application	Process-one	Ejabberd	2.0.0	beta1	All	All
Application	Process-one	Ejabberd	2.0.0	rc1	All	All
Application	Process-one	Ejabberd	2.0.1_2	All	All	All
Application	Process-one	Ejabberd	2.0.2	All	All	All
Application	Process-one	Ejabberd	2.0.3	All	All	All
Application	Process-one	Ejabberd	2.0.4	All	All	All
Application	Process-one	Ejabberd	2.0.5	All	All	All
Application	Process-one	Ejabberd	2.1.0	All	All	All
Application	Process-one	Ejabberd	2.1.1	All	All	All
Application	Process-one	Ejabberd	All	All	All	All

Vendor Declared Affected Products						
Source	Vendor	Product	Version		Platforms	
CNA	Na	N/a	affected n/a		Not specified	

References						
Reference					Source	
IBM X-Force Exchange					af854a3a-2127-422b-91ae-364da2661	
Debian -- Security Information -- DSA-2033-1 ejabberd					af854a3a-2127-422b-91ae-364da2661	
ejabberd Message Queue Denial of Service - Advisories - Community					af854a3a-2127-422b-91ae-364da2661	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH					af854a3a-2127-422b-91ae-364da2661	
[#EJAB-1173] ejabberd crashes when c2s message queue gets overloaded - ProcessOne - Support					af854a3a-2127-422b-91ae-364da2661	
oss-security - Re: CVE Request -- ejabberd					af854a3a-2127-422b-91ae-364da2661	
www.osvdb.org/62066					af854a3a-2127-422b-91ae-364da2661	
Debian update for ejabberd - Advisories - Community					af854a3a-2127-422b-91ae-364da2661	
ejabberd Idling/Stopped Message Remote Denial of Service Vulnerability					af854a3a-2127-422b-91ae-364da2661	

ejabberd client2server message Remote Denial of Service vulnerability	a1854a3a-2127-422b-91ae-364da2661
oss-security - CVE Request -- ejabberd	af854a3a-2127-422b-91ae-364da2661
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, 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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)