CVE-2013-6169

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2013-6169
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-10-17 23:55:00 UTC
Updated	2013-10-18 17:46:00 UTC
Description	The TLS driver in ejabberd before 2.1.12 supports (1) SSLv2 and (2) weak SSL ciphers, which makes it easier for remote a

Risk And Classification

Problem Types: CWE-310

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	2.1.10	All	All	All
Application	Process-one	Ejabberd	2.1.11	All	All	All
Application	Process-one	Ejabberd	2.1.2	All	All	All
Application	Process-one	Ejabberd	2.1.3	All	All	All
Application	Process-one	Ejabberd	2.1.4	All	All	All
Application	Process-one	Ejabberd	2.1.5	All	All	All
Application	Process-one	Ejabberd	2.1.6	All	All	All
Application	Process-one	Ejabberd	2.1.7	All	All	All
Application	Process-one	Ejabberd	2.1.8	All	All	All
Application	Process-one	Ejabberd	2.1.9	All	All	All
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	2.1.10	All	All	All
Application	Process-one	Ejabberd	2.1.11	All	All	All
Application	Process-one	Ejabberd	2.1.2	All	All	All
Application	Process-one	Ejabberd	2.1.3	All	All	All
Application	Process-one	Ejabberd	2.1.4	All	All	All
Application	Process-one	Ejabberd	2.1.5	All	All	All
Application	Process-one	Ejabberd	2.1.6	All	All	All
Application	Process-one	Ejabberd	2.1.7	All	All	All
Application	Process-one	Ejabberd	2.1.8	All	All	All
Application	Process-one	Ejabberd	2.1.9	All	All	All
Application	Process-one	Ejabberd	All	All	All	All

References

Reference	Source	Link	Tags
Debian -- Security Information -- DSA-2775-1 ejabberd	DEBIAN	www.debian.org	
Download ejabberd - World's Most Popular XMPP Application Server	CONFIRM	www.process-one.net	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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