CVE-2014-8760

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

Summary

CVE	CVE-2014-8760
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-10-25 00:55:00 UTC
Updated	2015-09-10 15:56:00 UTC
Description	ejabberd before 2.1.13 does not enforce the starttls_required setting when compression is used, which causes clients to es

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	All	All	All	All

References

Reference	Source	Link
Bug 1153839 – CVE-2014-8760 ejabberd: clients can unexpectedly connect without encryption	MISC	bugzilla.redhat.co
oss-sec: CVE request: ejabberd compression allows cirucumvention of encryption despite starttls_required	MLIST	seclists.org
Support / Security / Advisories / / MDVSA-2015:175 | Mandriva	MANDRIVA	www.mandriva.co
[Operators] ejabberd: compression allows circumvention of encryption	MLIST	mail.jabber.org
Mageia Advisory: MGASA-2014-0417 - Updated ejabberd packages fix security vulnerability	CONFIRM	advisories.mageia
Support / Security / Advisories / / MDVSA-2014:207 | Mandriva	MANDRIVA	www.mandriva.co
Make sure "starttls_required" can't be bypassed · processone/ejabberd@7bdc115 · GitHub	CONFIRM	github.com
ejabberd 'starttls_required' Encryption Security Weakness	BID	www.securityfocu
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**