CVE-2015-3420

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

Summary

CVE	CVE-2015-3420
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-09-19 15:29:00 UTC
Updated	2017-10-05 15:17:00 UTC
Description	The ssl-proxy-openssl.c function in Dovecot before 2.2.17, when SSLv3 is disabled, allow remote attackers to cause a deni

Risk And Classification

Problem Types: CWE-295

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Dovecot	Dovecot	All	All	All	All
Operating System	Fedoraproject	Fedora	20	All	All	All
Operating System	Fedoraproject	Fedora	21	All	All	All
Operating System	Fedoraproject	Fedora	22	All	All	All
Operating System	Fedoraproject	Fedora	20	All	All	All
Operating System	Fedoraproject	Fedora	21	All	All	All
Operating System	Fedoraproject	Fedora	22	All	All	All

References

Reference	Source	Li
[Dovecot-news] v2.2.17 released	MLIST	do
oss-security - Re: Re: CVE request: Dovecot remote DoS on TLS connections	MLIST	ww
[SECURITY] Fedora 22 Update: dovecot-2.2.16-2.fc22	FEDORA	lis
oss-security - Re: CVE request: Dovecot remote DoS on TLS connections	MLIST	ww
[patch] TLS Handshake failures can crash imap-login	MLIST	do
[SECURITY] Fedora 20 Update: dovecot-2.2.16-2.fc20	FEDORA	lis
[SECURITY] Fedora 21 Update: dovecot-2.2.16-2.fc21	FEDORA	lis

1216057 – (CVE-2015-3420) CVE-2015-3420 dovecot: SSL/TLS handshake failures leading to a crash of the login process.	CONFIRM	bu
Dovecot 'ssl-proxy-openssl.c' Remote Denial of Service Vulnerability	BID	ww
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nv

No vendor comments have been submitted for this CVE.

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