CVE-2013-2111

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

Summary

CVE	CVE-2013-2111
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-05-27 14:55:00 UTC
Updated	2014-05-28 16:25:00 UTC
Description	The IMAP functionality in Dovecot before 2.2.2 allows remote attackers to cause a denial of service (infinite loop and CPU c

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Dovecot	Dovecot	2.2	rc1	All	All
Application	Dovecot	Dovecot	2.2	rc2	All	All
Application	Dovecot	Dovecot	2.2	rc3	All	All
Application	Dovecot	Dovecot	2.2	rc4	All	All
Application	Dovecot	Dovecot	2.2	rc5	All	All
Application	Dovecot	Dovecot	2.2	rc6	All	All
Application	Dovecot	Dovecot	2.2	rc7	All	All
Application	Dovecot	Dovecot	2.2.0	All	All	All
Application	Dovecot	Dovecot	2.2	rc1	All	All
Application	Dovecot	Dovecot	2.2	rc2	All	All
Application	Dovecot	Dovecot	2.2	rc3	All	All
Application	Dovecot	Dovecot	2.2	rc4	All	All
Application	Dovecot	Dovecot	2.2	rc5	All	All
Application	Dovecot	Dovecot	2.2	rc6	All	All
Application	Dovecot	Dovecot	2.2	rc7	All	All
Application	Dovecot	Dovecot	2.2.0	All	All	All
Application	Dovecot	Dovecot	All	All	All	All

References

Reference	Source	Link
Dovecot APPEND Parameter Processing Flaw Lets Remote Authenticated Users Deny Service - SecurityTracker	SECTRACK	www.secur
oss-security - Re: CVE request: dovecot : "APPEND" Parameters Processing Denial of Service Vulnerability	MLIST	www.open
[Dovecot-news] v2.2.2 released	MLIST	www.dove
About Secunia Research | Flexera	SECUNIA	secunia.co
CVE Program record	CVE.ORG	www.cve.o
NVD vulnerability detail	NVD	nvd.nist.go

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**