CVE-2011-1926

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

Summary

CVE	CVE-2011-1926
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-05-23 22:55:01 UTC
Updated	2026-04-29 01:13:23 UTC
Description	The STARTTLS implementation in Cyrus IMAP Server before 2.4.7 does not properly restrict I/O buffering, which allows ma

Risk And Classification

Primary CVSS: v2.0 5.1 from nvd@nist.gov

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

Problem Types: CWE-264 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

High

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cmu	Cyrus Imap Server	2.0.17	All	All	All

Application	Cmu	Cyrus Imap Server	2.1.16	All	All	All
Application	Cmu	Cyrus Imap Server	2.1.17	All	All	All
Application	Cmu	Cyrus Imap Server	2.1.18	All	All	All
Application	Cmu	Cyrus Imap Server	2.2.10	All	All	All
Application	Cmu	Cyrus Imap Server	2.2.11	All	All	All
Application	Cmu	Cyrus Imap Server	2.2.12	All	All	All
Application	Cmu	Cyrus Imap Server	2.2.13	All	All	All
Application	Cmu	Cyrus Imap Server	2.2.13p1	All	All	All
Application	Cmu	Cyrus Imap Server	2.2.8	All	All	All
Application	Cmu	Cyrus Imap Server	2.2.9	All	All	All
Application	Cmu	Cyrus Imap Server	2.3.0	All	All	All
Application	Cmu	Cyrus Imap Server	2.3.1	All	All	All
Application	Cmu	Cyrus Imap Server	2.3.10	All	All	All
Application	Cmu	Cyrus Imap Server	2.3.11	All	All	All
Application	Cmu	Cyrus Imap Server	2.3.12	All	All	All
Application	Cmu	Cyrus Imap Server	2.3.13	All	All	All
Application	Cmu	Cyrus Imap Server	2.3.14	All	All	All
Application	Cmu	Cyrus Imap Server	2.3.15	All	All	All
Application	Cmu	Cyrus Imap Server	2.3.16	All	All	All
Application	Cmu	Cyrus Imap Server	2.3.2	All	All	All
Application	Cmu	Cyrus Imap Server	2.3.3	All	All	All
Application	Cmu	Cyrus Imap Server	2.3.4	All	All	All
Application	Cmu	Cyrus Imap Server	2.3.5	All	All	All
Application	Cmu	Cyrus Imap Server	2.3.6	All	All	All
Application	Cmu	Cyrus Imap Server	2.3.7	All	All	All
Application	Cmu	Cyrus Imap Server	2.3.8	All	All	All
Application	Cmu	Cyrus Imap Server	2.3.9	All	All	All
Application	Cmu	Cyrus Imap Server	2.4.0	All	All	All
Application	Cmu	Cyrus Imap Server	2.4.1	All	All	All
Application	Cmu	Cyrus Imap Server	2.4.2	All	All	All
Application	Cmu	Cyrus Imap Server	2.4.3	All	All	All
Application	Cmu	Cyrus Imap Server	2.4.4	All	All	All
Application	Cmu	Cyrus Imap Server	2.4.5	All	All	All
Application	Cmu	Cyrus Imap Server	All	All	All	All

Vendor Declared Affected Products

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

References

Reference
IBM X-Force Exchange
No page found
Support
Debian -- Security Information -- DSA-2258-1 kolab-cyrus-imapd
oss-security - CVE Request -- Cyrus-IMAP STARTTLS issue -- [was: Re: pure-ftpd STARTTLS command injection / new CVE?]
No page found
No page found
[SECURITY] Fedora 14 Update: cyrus-imapd-2.3.16-8.fc14
Project Cyrus
Support / Security / Advisories / / MDVSA-2011:100 | Mandriva
Debian update for kolab-cyrus-imapd - Secunia.com
Red Hat update for cyrus-imapd - Secunia.com
Cyrus IMAP Server STARTTLS Buffer Flushing Flaw Lets Remote Users Inject Commands via Man-in-the-Middle Attacks - SecurityTracker
705288 – (CVE-2011-1926) CVE-2011-1926 cyrus-imapd: STARTTLS plaintext command injection
oss-security - Re: CVE Request -- Cyrus-IMAP STARTTLS issue -- [was: Re: pure-ftpd STARTTLS command injection / new CVE?]
Debian update for cyrus-imapd-2.2 - Secunia.com
US-CERT Vulnerability Note VU#555316 - STARTTLS plaintext command injection vulnerability
Debian -- Security Information -- DSA-2242-1 cyrus-imapd-2.2
[SECURITY] Fedora 13 Update: cyrus-imapd-2.3.16-5.fc13
Fedora update for cyrus-imapd - Secunia.com
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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