CVE-2013-4122

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

Summary

CVE	CVE-2013-4122
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-10-27 00:55:03 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Cyrus SASL 2.1.23, 2.1.26, and earlier does not properly handle when a NULL value is returned upon an error by the crypt

Risk And Classification

Primary CVSS: v2.0 4.3 from nvd@nist.gov

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

Problem Types: CWE-189 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cmu	Cyrus-sasl	1.5.28	All	All	All

Application	Cmu	Cyrus-sasl	2.1.19	All	All	All
Application	Cmu	Cyrus-sasl	2.1.20	All	All	All
Application	Cmu	Cyrus-sasl	2.1.21	All	All	All
Application	Cmu	Cyrus-sasl	2.1.22	All	All	All
Application	Cmu	Cyrus-sasl	2.1.23	All	All	All
Application	Cmu	Cyrus-sasl	2.1.24	All	All	All
Application	Cmu	Cyrus-sasl	2.1.25	All	All	All
Application	Cmu	Cyrus-sasl	All	All	All	All
Application	Gnu	Glibc	2.17	All	All	All
Application	Gnu	Glibc	2.18	All	All	All
Application	Gnu	Glibc	2.2	All	All	All
Application	Gnu	Glibc	2.2.1	All	All	All
Application	Gnu	Glibc	2.2.2	All	All	All
Application	Gnu	Glibc	2.2.3	All	All	All
Application	Gnu	Glibc	2.2.4	All	All	All
Application	Gnu	Glibc	2.2.5	All	All	All
Application	Gnu	Glibc	2.3	All	All	All
Application	Gnu	Glibc	2.3.1	All	All	All
Application	Gnu	Glibc	2.3.10	All	All	All
Application	Gnu	Glibc	2.3.2	All	All	All
Application	Gnu	Glibc	2.3.3	All	All	All
Application	Gnu	Glibc	2.3.4	All	All	All
Application	Gnu	Glibc	2.3.5	All	All	All
Application	Gnu	Glibc	2.3.6	All	All	All
Application	Gnu	Glibc	2.4	All	All	All
Application	Gnu	Glibc	2.5	All	All	All
Application	Gnu	Glibc	2.5.1	All	All	All
Application	Gnu	Glibc	2.6	All	All	All
Application	Gnu	Glibc	2.6.1	All	All	All
Application	Gnu	Glibc	2.7	All	All	All
Application	Gnu	Glibc	2.8	All	All	All
Application	Gnu	Glibc	2.9	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source	Link	T
oss-security - CVE request: Cyrus-sasl NULL ptr. dereference	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com	
oss-security - Re: CVE request: Cyrus-sasl NULL ptr. dereference	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com	
oss-security - Re: CVE request: Cyrus-sasl NULL ptr. dereference	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com	
[Slackware-current] glibc 2.17, shadow, and other penumbrae	af854a3a-2127-422b-91ae-364da2661108	www.linuxquestions.org	
No page found	af854a3a-2127-422b-91ae-364da2661108	git.cyrusimap.org	E
Debian -- Security Information -- DSA-3368-1 cyrus-sasl2	af854a3a-2127-422b-91ae-364da2661108	www.debian.org	
USN-2755-1: Cyrus SASL vulnerability | Ubuntu	af854a3a-2127-422b-91ae-364da2661108	www.ubuntu.com	
Gentoo Linux Documentation -- Cyrus-SASL: Denial of Service	af854a3a-2127-422b-91ae-364da2661108	security.gentoo.org	
oss-security - Re: CVE request: Cyrus-sasl NULL ptr. dereference	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com	
CVE Program record	CVE.ORG	www.cve.org	c
NVD vulnerability detail	NVD	nvd.nist.gov	c

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

500140 Alpine Linux Security Update for cyrus-sasl

503790 Alpine Linux Security Update for cyrus-sasl