CVE-2014-2892

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

Summary

CVE	CVE-2014-2892
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-04-22 14:23:35 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Heap-based buffer overflow in the get_answer function in mmsh.c in libmms before 0.6.4 allows remote attackers to execut

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

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

Problem Types: CWE-119 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Libmms Project	Libmms	0.6	All	All	All

Application	Libmms Project	Libmms	0.6.1	All	All	All
Application	Libmms Project	Libmms	0.6.2	All	All	All
Application	Libmms Project	Libmms	All	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
IBM X-Force Exchange	af854a3a-2127-422b-91ae-3
Security Advisory SA57875 - libmms MMSH Server Response Parsing Buffer Overflow Vulnerability - Secunia	af854a3a-2127-422b-91ae-3
libmms: Remote execution of arbitrary code (GLSA 201612-29) — Gentoo security	af854a3a-2127-422b-91ae-3
oss-security - Re: libmms heap-based buffer overflow fix	af854a3a-2127-422b-91ae-3
libmms / Code / Commit [03bcfc]	af854a3a-2127-422b-91ae-3
Debian -- Security Information -- DSA-2916-1 libmms	af854a3a-2127-422b-91ae-3
openSUSE-SU-2014:0590-1: moderate: update for libmms	af854a3a-2127-422b-91ae-3
libmms / Code / [a9f692] /ChangeLog	af854a3a-2127-422b-91ae-3
libmms MMSH Server Response Heap-Based Buffer Overflow Vulnerability	af854a3a-2127-422b-91ae-3
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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