CVE-2012-4409

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

Summary

CVE	CVE-2012-4409
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-11-21 23:55:01 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Stack-based buffer overflow in the check_file_head function in extra.c in mcrypt 2.6.8 and earlier allows user-assisted remo

Risk And Classification

Primary CVSS: v2.0 6.8 from nvd@nist.gov

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

Problem Types: CWE-119 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mcrypt	Mcrypt	2.6.4	All	All	All

Application	Mcrypt	Mcrypt	2.6.5	All	All	All
Application	Mcrypt	Mcrypt	2.6.6	All	All	All
Application	Mcrypt	Mcrypt	2.6.7	All	All	All
Application	Mcrypt	Mcrypt	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
mcrypt 2.6.8 Buffer Overflow Proof Of Concept ≈ Packet Storm	af854a3a-2127-422b-91ae-364da2661108
oss-security - Re: CVE request - mcrypt buffer overflow flaw	af854a3a-2127-422b-91ae-364da2661108
[SECURITY] Fedora 17 Update: mcrypt-2.6.8-9.fc17	af854a3a-2127-422b-91ae-364da2661108
[SECURITY] Fedora 18 Update: mcrypt-2.6.8-9.fc18	af854a3a-2127-422b-91ae-364da2661108
About Secunia Research | Flexera	af854a3a-2127-422b-91ae-364da2661108
Security Advisory SA51010 - SUSE update for mcrypt - Secunia	af854a3a-2127-422b-91ae-364da2661108
[SECURITY] Fedora 16 Update: mcrypt-2.6.8-9.fc16	af854a3a-2127-422b-91ae-364da2661108
Bug 855029 – CVE-2012-4409 mcrypt: buffer overflow when processing encrypted file headers	af854a3a-2127-422b-91ae-364da2661108
MCrypt Stack Overflow Lets Remote Users Execute Arbitrary Code - SecurityTracker	af854a3a-2127-422b-91ae-364da2661108
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.