CVE-2008-4201

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

Summary

CVE	CVE-2008-4201
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-09-24 11:42:00 UTC
Updated	2011-01-03 05:00:00 UTC
Description	Heap-based buffer overflow in the decodeMP4file function (frontend/main.c) in FAAD2 2.6.1 and earlier allows remote attac

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Audiocoding	Faad2	1.1	All	All	All
Application	Audiocoding	Faad2	2.0	rc1	All	All
Application	Audiocoding	Faad2	2.0	rc2	All	All
Application	Audiocoding	Faad2	2.0	rc3	All	All
Application	Audiocoding	Faad2	2.5	All	All	All
Application	Audiocoding	Faad2	1.1	All	All	All
Application	Audiocoding	Faad2	2.0	rc1	All	All
Application	Audiocoding	Faad2	2.0	rc2	All	All
Application	Audiocoding	Faad2	2.0	rc3	All	All
Application	Audiocoding	Faad2	2.5	All	All	All
Application	Audiocoding	Faad2	All	All	All	All

References

Reference	Source	Link
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vup
FAAD2 Frontend 'decodeMP4file()' Heap Based Buffer Overflow Vulnerability	BID	www.sec
bugs.gentoo.org/attachment.cgi	MISC	bugs.ger

Faad2 "decodeMP4file()" Buffer Overflow Vulnerability - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia.c
AudioCoding.com - Archive	CONFIRM	www.auc
48349	OSVDB	osvdb.or
oss-security - Re: CVE id request: fraud2	MLIST	www.ope
Gentoo Linux Documentation -- FAAD2: User-assisted execution of arbitrary code	GENTOO	security.g
Gentoo Bug 238445 - media-libs/faad2 < 2.6.1-r2: heap overflow in the frontend (CVE-2008-4201)	CONFIRM	bugs.ger
Gentoo update for faad2 - Secunia.com	SECUNIA	secunia.c
#499899 - fraad2: heap overflow - Debian Bug report logs	CONFIRM	bugs.deb
www.audiocoding.com/patch/main_overflow.diff	CONFIRM	www.auc
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.g

No vendor comments have been submitted for this CVE.

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