CVE-2011-3362

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

Summary

CVE	CVE-2011-3362
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-10-02 20:55:01 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Integer signedness error in the decode_residual_block function in cavsdec.c in libavcodec in FFmpeg before 0.7.3 and 0.8.x

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-189 | 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	Ffmpeg	Ffmpeg	0.3	All	All	All

Application	Ffmpeg	Ffmpeg	0.3.1	All	All	All
Application	Ffmpeg	Ffmpeg	0.3.2	All	All	All
Application	Ffmpeg	Ffmpeg	0.3.3	All	All	All
Application	Ffmpeg	Ffmpeg	0.3.4	All	All	All
Application	Ffmpeg	Ffmpeg	0.4.0	All	All	All
Application	Ffmpeg	Ffmpeg	0.4.2	All	All	All
Application	Ffmpeg	Ffmpeg	0.4.3	All	All	All
Application	Ffmpeg	Ffmpeg	0.4.4	All	All	All
Application	Ffmpeg	Ffmpeg	0.4.5	All	All	All
Application	Ffmpeg	Ffmpeg	0.4.6	All	All	All
Application	Ffmpeg	Ffmpeg	0.4.7	All	All	All
Application	Ffmpeg	Ffmpeg	0.4.8	All	All	All
Application	Ffmpeg	Ffmpeg	0.4.9	pre1	All	All
Application	Ffmpeg	Ffmpeg	0.5	All	All	All
Application	Ffmpeg	Ffmpeg	0.5.1	All	All	All
Application	Ffmpeg	Ffmpeg	0.5.2	All	All	All
Application	Ffmpeg	Ffmpeg	0.5.3	All	All	All
Application	Ffmpeg	Ffmpeg	0.5.4	All	All	All
Application	Ffmpeg	Ffmpeg	0.6	All	All	All
Application	Ffmpeg	Ffmpeg	0.6.1	All	All	All
Application	Ffmpeg	Ffmpeg	0.6.2	All	All	All
Application	Ffmpeg	Ffmpeg	0.7.1	All	All	All
Application	Ffmpeg	Ffmpeg	0.8.0	All	All	All
Application	Ffmpeg	Ffmpeg	0.8.1	All	All	All
Application	Ffmpeg	Ffmpeg	All	All	All	All
Application	Libav	Libav	0.3	All	All	All
Application	Libav	Libav	0.3.1	All	All	All
Application	Libav	Libav	0.3.2	All	All	All
Application	Libav	Libav	0.3.3	All	All	All
Application	Libav	Libav	0.3.4	All	All	All
Application	Libav	Libav	0.4.0	All	All	All
Application	Libav	Libav	0.4.1	All	All	All
Application	Libav	Libav	0.4.2	All	All	All
Application	Libav	Libav	0.4.3	All	All	All
Application	Libav	Libav	0.4.4	All	All	All
Application	Libav	Libav	0.4.5	All	All	All

Application	Libav	Libav	0.4.6	All	All	All
Application	Libav	Libav	0.4.7	All	All	All
Application	Libav	Libav	0.4.8	All	All	All
Application	Libav	Libav	0.4.9	pre1	All	All
Application	Libav	Libav	0.5	All	All	All
Application	Libav	Libav	0.5.4	All	All	All
Application	Libav	Libav	0.6	All	All	All
Application	Libav	Libav	0.6.1	All	All	All
Application	Libav	Libav	0.6.2	All	All	All
Application	Libav	Libav	0.7	beta1	All	All
Application	Libav	Libav	0.7	beta2	All	All
Application	Libav	Libav	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	L
www.ffmpeg.org/releases/ffmpeg-0.8.4.changelog	af854a3a-2127-422b-91ae-364da2661108	w
git.videolan.org Git - ffmpeg.git/commit	af854a3a-2127-422b-91ae-364da2661108	g
www.ffmpeg.org/releases/ffmpeg-0.7.5.changelog	af854a3a-2127-422b-91ae-364da2661108	w
oss-security - Re: CVE request: ffmpeg/libav insufficuent boundary check in CAVS decoding	af854a3a-2127-422b-91ae-364da2661108	w
FFmpeg Multiple Vulnerabilities - Secunia.com	af854a3a-2127-422b-91ae-364da2661108	s
oss-security - CVE request: ffmpeg/libav insufficuent boundary check in CAVS decoding	af854a3a-2127-422b-91ae-364da2661108	w
oCERT.org - oCERT Advisories	af854a3a-2127-422b-91ae-364da2661108	w
git.videolan.org Git - ffmpeg.git/commit	af854a3a-2127-422b-91ae-364da2661108	g
git.videolan.org Git - ffmpeg.git/commit	MITRE	g
git.videolan.org Git - ffmpeg.git/commit	MITRE	g
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	n

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report