CVE-2017-9996

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

Summary

CVE	CVE-2017-9996
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-06-28 06:29:00 UTC
Updated	2017-07-05 14:54:00 UTC
Description	The cdxl_decode_frame function in libavcodec/cdxl.c in FFmpeg 2.8.x before 2.8.12, 3.0.x before 3.0.8, 3.1.x before 3.1.8,

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ffmpeg	Ffmpeg	2.8	All	All	All
Application	Ffmpeg	Ffmpeg	2.8.1	All	All	All
Application	Ffmpeg	Ffmpeg	2.8.10	All	All	All
Application	Ffmpeg	Ffmpeg	2.8.11	All	All	All
Application	Ffmpeg	Ffmpeg	2.8.2	All	All	All
Application	Ffmpeg	Ffmpeg	2.8.3	All	All	All
Application	Ffmpeg	Ffmpeg	2.8.4	All	All	All
Application	Ffmpeg	Ffmpeg	2.8.5	All	All	All
Application	Ffmpeg	Ffmpeg	2.8.6	All	All	All
Application	Ffmpeg	Ffmpeg	2.8.7	All	All	All
Application	Ffmpeg	Ffmpeg	2.8.8	All	All	All
Application	Ffmpeg	Ffmpeg	2.8.9	All	All	All
Application	Ffmpeg	Ffmpeg	3.0	All	All	All
Application	Ffmpeg	Ffmpeg	3.0.1	All	All	All
Application	Ffmpeg	Ffmpeg	3.0.2	All	All	All
Application	Ffmpeg	Ffmpeg	3.0.3	All	All	All
Application	Ffmpeg	Ffmpeg	3.0.4	All	All	All

Application	Ffmpeg	Ffmpeg	3.0.5	All	All	All
Application	Ffmpeg	Ffmpeg	3.0.6	All	All	All
Application	Ffmpeg	Ffmpeg	3.0.7	All	All	All
Application	Ffmpeg	Ffmpeg	3.1	All	All	All
Application	Ffmpeg	Ffmpeg	3.1.1	All	All	All
Application	Ffmpeg	Ffmpeg	3.1.2	All	All	All
Application	Ffmpeg	Ffmpeg	3.1.3	All	All	All
Application	Ffmpeg	Ffmpeg	3.1.4	All	All	All
Application	Ffmpeg	Ffmpeg	3.1.5	All	All	All
Application	Ffmpeg	Ffmpeg	3.1.6	All	All	All
Application	Ffmpeg	Ffmpeg	3.1.7	All	All	All
Application	Ffmpeg	Ffmpeg	3.2	All	All	All
Application	Ffmpeg	Ffmpeg	3.2.1	All	All	All
Application	Ffmpeg	Ffmpeg	3.2.2	All	All	All
Application	Ffmpeg	Ffmpeg	3.2.3	All	All	All
Application	Ffmpeg	Ffmpeg	3.2.4	All	All	All
Application	Ffmpeg	Ffmpeg	3.3	All	All	All
Application	Ffmpeg	Ffmpeg	2.8	All	All	All
Application	Ffmpeg	Ffmpeg	2.8.1	All	All	All
Application	Ffmpeg	Ffmpeg	2.8.10	All	All	All
Application	Ffmpeg	Ffmpeg	2.8.11	All	All	All
Application	Ffmpeg	Ffmpeg	2.8.2	All	All	All
Application	Ffmpeg	Ffmpeg	2.8.3	All	All	All
Application	Ffmpeg	Ffmpeg	2.8.4	All	All	All
Application	Ffmpeg	Ffmpeg	2.8.5	All	All	All
Application	Ffmpeg	Ffmpeg	2.8.6	All	All	All
Application	Ffmpeg	Ffmpeg	2.8.7	All	All	All
Application	Ffmpeg	Ffmpeg	2.8.8	All	All	All
Application	Ffmpeg	Ffmpeg	2.8.9	All	All	All
Application	Ffmpeg	Ffmpeg	3.0	All	All	All
Application	Ffmpeg	Ffmpeg	3.0.1	All	All	All
Application	Ffmpeg	Ffmpeg	3.0.2	All	All	All
Application	Ffmpeg	Ffmpeg	3.0.3	All	All	All
Application	Ffmpeg	Ffmpeg	3.0.4	All	All	All
Application	Ffmpeg	Ffmpeg	3.0.5	All	All	All

Application	Ffmpeg	Ffmpeg	3.0.6	All	All	All
Application	Ffmpeg	Ffmpeg	3.0.7	All	All	All
Application	Ffmpeg	Ffmpeg	3.1	All	All	All
Application	Ffmpeg	Ffmpeg	3.1.1	All	All	All
Application	Ffmpeg	Ffmpeg	3.1.2	All	All	All
Application	Ffmpeg	Ffmpeg	3.1.3	All	All	All
Application	Ffmpeg	Ffmpeg	3.1.4	All	All	All
Application	Ffmpeg	Ffmpeg	3.1.5	All	All	All
Application	Ffmpeg	Ffmpeg	3.1.6	All	All	All
Application	Ffmpeg	Ffmpeg	3.1.7	All	All	All
Application	Ffmpeg	Ffmpeg	3.2	All	All	All
Application	Ffmpeg	Ffmpeg	3.2.1	All	All	All
Application	Ffmpeg	Ffmpeg	3.2.2	All	All	All
Application	Ffmpeg	Ffmpeg	3.2.3	All	All	All
Application	Ffmpeg	Ffmpeg	3.2.4	All	All	All
Application	Ffmpeg	Ffmpeg	3.3	All	All	All

References

Reference	Source	Link	Tags
FFmpeg CVE-2017-9996 Heap Buffer Overflow Vulnerability	BID	www.securityfocus.com	Third Party Advisory,
avcodec/cdxl: Check format parameter · FFmpeg/FFmpeg@e1b60aa · GitHub	MISC	github.com	Issue Tracking, Patch
avcodec/cdxl: Check format for BGR24 · FFmpeg/FFmpeg@1e42736 · GitHub	MISC	github.com	Issue Tracking, Patch
1427 - oss-fuzz - OSS-Fuzz: Fuzzing the planet - Monorail	MISC	bugs.chromium.org	Issue Tracking, Third
1378 - oss-fuzz - OSS-Fuzz: Fuzzing the planet - Monorail	MISC	bugs.chromium.org	Issue Tracking, Third
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

site. This site includes MITRE data granted under the following license.

Free CVE JSON API cve.report/api

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