



CVE-2012-0947

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2012-0947
State	PUBLIC
Assigner	security@ubuntu.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-08-20 18:55:00 UTC
Updated	2023-11-07 02:10:00 UTC
Description	Heap-based buffer overflow in the vqa_decode_chunk function in the VQA codec (vqavideo.c) in libavcodec in Libav 0.5.x k

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Libav	Libav	0.5	All	All	All
Application	Libav	Libav	0.5.1	All	All	All
Application	Libav	Libav	0.5.2	All	All	All
Application	Libav	Libav	0.5.3	All	All	All
Application	Libav	Libav	0.5.4	All	All	All
Application	Libav	Libav	0.5.5	All	All	All
Application	Libav	Libav	0.5.6	All	All	All
Application	Libav	Libav	0.5.7	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	0.6.3	All	All	All
Application	Libav	Libav	0.6.4	All	All	All
Application	Libav	Libav	0.6.5	All	All	All
Application	Libav	Libav	0.7	All	All	All
Application	Libav	Libav	0.7	beta1	All	All
Application	Libav	Libav	0.7	beta2	All	All

Application	Libav	Libav	0.7.1	All	All	All
Application	Libav	Libav	0.7.2	All	All	All
Application	Libav	Libav	0.7.3	All	All	All
Application	Libav	Libav	0.7.4	All	All	All
Application	Libav	Libav	0.7.5	All	All	All
Application	Libav	Libav	0.8	All	All	All
Application	Libav	Libav	0.8	beta2	All	All
Application	Libav	Libav	0.8.1	All	All	All
Application	Libav	Libav	0.5	All	All	All
Application	Libav	Libav	0.5.1	All	All	All
Application	Libav	Libav	0.5.2	All	All	All
Application	Libav	Libav	0.5.3	All	All	All
Application	Libav	Libav	0.5.4	All	All	All
Application	Libav	Libav	0.5.5	All	All	All
Application	Libav	Libav	0.5.6	All	All	All
Application	Libav	Libav	0.5.7	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	0.6.3	All	All	All
Application	Libav	Libav	0.6.4	All	All	All
Application	Libav	Libav	0.6.5	All	All	All
Application	Libav	Libav	0.7	All	All	All
Application	Libav	Libav	0.7	beta1	All	All
Application	Libav	Libav	0.7	beta2	All	All
Application	Libav	Libav	0.7.1	All	All	All
Application	Libav	Libav	0.7.2	All	All	All
Application	Libav	Libav	0.7.3	All	All	All
Application	Libav	Libav	0.7.4	All	All	All
Application	Libav	Libav	0.7.5	All	All	All
Application	Libav	Libav	0.8	All	All	All
Application	Libav	Libav	0.8	beta2	All	All
Application	Libav	Libav	0.8.1	All	All	All

Reference	Source	Link	Tags
Bug #980963 "Heap-based Buffer Overflow in libavcodec" : Bugs : libav package : Ubuntu	MISC	bugs.launchpad.net	Exploit
Libav	CONFIRM	libav.org	
git.libav.org Git - libav.git/commit	CONFIRM	git.libav.org	Patch
oss-security - Security issue in libav/ffmpeg	MLIST	www.openwall.com	
USN-1479-1: FFmpeg vulnerabilities Ubuntu	UBUNTU	www.ubuntu.com	
FFmpeg libavcodec 'vqavideo.c' '.vaq' File Heap Memory Corruption Vulnerability	BID	www.securityfocus.com	
Security Alerts - Secunia	SECUNIA	secunia.com	
git.libav.org Git - libav.git/commit		git.libav.org	
Debian -- Security Information -- DSA-2471-1 ffmpeg	DEBIAN	www.debian.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org). This site includes MITRE data granted under the following [license](https://www.mitre.org).

Free CVE JSON API cve.report/api

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