



CVE-2010-4704

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

Summary

CVE	CVE-2010-4704
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-01-22 22:00:00 UTC
Updated	2023-11-07 02:06:00 UTC
Description	libavcodec/vorbis_dec.c in the Vorbis decoder in FFmpeg 0.6.1 and earlier allows remote attackers to cause a denial of ser

Risk And Classification

Problem Types: CWE-20

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	0.6	All	All	All
Application	Ffmpeg	Ffmpeg	All	All	All	All

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	0.6	All	All	All

References						
Reference	Source	Link	Tags			
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com				
Support / Security / Advisories // MDVSA-2011:114 Mandriva	MANDRIVA	www.mandriva.com				
Support / Security / Advisories // MDVSA-2011:089 Mandriva	MANDRIVA	www.mandriva.com				
Support / Security / Advisories // MDVSA-2011:088 Mandriva	MANDRIVA	www.mandriva.com				
FFmpeg	CONFIRM	ffmpeg.mplayerhq.hu				
Debian -- Security Information -- DSA-2165-1 ffmpeg-debian	DEBIAN	www.debian.org				
FFmpeg Integer Overflow and Denial of Service Vulnerabilities	BID	www.securityfocus.com				
FFmpeg	CONFIRM	git.ffmpeg.org	Patch			
Support / Security / Advisories // MDVSA-2011:061 Mandriva	MANDRIVA	www.mandriva.com				
Support / Security / Advisories // MDVSA-2011:060 Mandriva	MANDRIVA	www.mandriva.com				
Support / Security / Advisories // MDVSA-2011:062 Mandriva	MANDRIVA	www.mandriva.com				
Support / Security / Advisories // MDVSA-2011:112 Mandriva	MANDRIVA	www.mandriva.com				
USN-1104-1: FFmpeg vulnerabilities Ubuntu	UBUNTU	www.ubuntu.com				
FFmpeg		git.ffmpeg.org				
Debian update for ffmpeg-debian - Advisories - Community	SECUNIA	secunia.com				
404 Not Found	CONFIRM	roundup.ffmpeg.org	Exploit			
Debian -- Security Information -- DSA-2002-14	DEBIAN	www.debian.org				

Debian -- Security Information -- DSA-2306-1 ffmpeg	DEBIAN	www.debian.org	
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.			

© [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](#) and the authoritative source of CVE content is [MITRE's CVE web 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