



CVE-2017-10699

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

Summary

CVE	CVE-2017-10699
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-06-30 13:29:00 UTC
Updated	2017-11-23 02:29:00 UTC
Description	avcodec 2.2.x, as used in VideoLAN VLC media player 2.2.7-x before 2017-06-29, allows out-of-bounds heap memory write

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Videolan	Vlc Media Player	2.2.0	All	All	All
Application	Videolan	Vlc Media Player	2.2.1	All	All	All
Application	Videolan	Vlc Media Player	2.2.2	All	All	All
Application	Videolan	Vlc Media Player	2.2.3	All	All	All
Application	Videolan	Vlc Media Player	2.2.4	All	All	All
Application	Videolan	Vlc Media Player	2.2.5	All	All	All
Application	Videolan	Vlc Media Player	2.2.5.1	All	All	All
Application	Videolan	Vlc Media Player	2.2.6	All	All	All
Application	Videolan	Vlc Media Player	2.2.7	All	All	All
Application	Videolan	Vlc Media Player	2.2.0	All	All	All
Application	Videolan	Vlc Media Player	2.2.1	All	All	All
Application	Videolan	Vlc Media Player	2.2.2	All	All	All
Application	Videolan	Vlc Media Player	2.2.3	All	All	All
Application	Videolan	Vlc Media Player	2.2.4	All	All	All
Application	Videolan	Vlc Media Player	2.2.5	All	All	All
Application	Videolan	Vlc Media Player	2.2.5.1	All	All	All
Application	Videolan	Vlc Media Player	2.2.6	All	All	All

Application	Videolan	Vlc Media Player	2.2.7	All	All	All
References						
Reference						
VLC Media Player File Processing Out-of-Bounds Memory Write Error in avcodec Component May Let Remote Users Execute Arbitrary Code						
Debian -- Security Information -- DSA-4045-1 vlc						
#18467 (VLC Windows 2.2.7 Crash due to Out-of-Bound Heap Memory Write) – VLC						
CVE Program record						
NVD vulnerability detail						
No vendor comments have been submitted for this CVE.						
There are currently no legacy QID mappings associated with this CVE.						

© [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](#)