



CVE-2011-1684

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

Summary

CVE	CVE-2011-1684
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-05-03 20:55:11 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Heap-based buffer overflow in the MP4_ReadBox_skr function in libmp4.c in the MP4 demultiplexer in VideoLAN VLC me...

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-119 | 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	Videolan	Vlc Media Player	1.0.0	All	All	All

Application	Videolan	Vlc Media Player	1.0.1	All	All	All
Application	Videolan	Vlc Media Player	1.0.2	All	All	All
Application	Videolan	Vlc Media Player	1.0.3	All	All	All
Application	Videolan	Vlc Media Player	1.0.4	All	All	All
Application	Videolan	Vlc Media Player	1.0.5	All	All	All
Application	Videolan	Vlc Media Player	1.0.6	All	All	All
Application	Videolan	Vlc Media Player	1.1.0	All	All	All
Application	Videolan	Vlc Media Player	1.1.1	All	All	All
Application	Videolan	Vlc Media Player	1.1.2	All	All	All
Application	Videolan	Vlc Media Player	1.1.3	All	All	All
Application	Videolan	Vlc Media Player	1.1.4	All	All	All
Application	Videolan	Vlc Media Player	1.1.5	All	All	All
Application	Videolan	Vlc Media Player	1.1.6	All	All	All
Application	Videolan	Vlc Media Player	1.1.6.1	All	All	All
Application	Videolan	Vlc Media Player	1.1.7	All	All	All
Application	Videolan	Vlc Media Player	1.1.8	All	All	All

Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		

References						
Reference					Source	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH					af854a3a-2127-42	
oss-security - Re: CVE id request: vlc					af854a3a-2127-42	
oss-security - Re: CVE id request: vlc					af854a3a-2127-42	
VLC Media Player "MP4_ReadBox_skcr()" Buffer Overflow Vulnerability - Secunia.com					af854a3a-2127-42	
IBM X-Force Exchange					af854a3a-2127-42	
VLC Media Player 'MP4' Heap Based Buffer Overflow Vulnerability					af854a3a-2127-42	
oss-security - CVE id request: vlc					af854a3a-2127-42	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH					af854a3a-2127-42	
Debian update for vlc - Secunia.com					af854a3a-2127-42	
git.videolan.org Git - vlc.git/commit					af854a3a-2127-42	
VLC Media Player Heap Overflow in MP4_ReadBox_skcr() Lets Remote Users Execute Arbitrary Code - SecurityTracker					af854a3a-2127-42	
VideoLAN - VideoLAN Security Advisory 1103					af854a3a-2127-42	
Debian -- Security Information -- DSA-2218-1 vlc					af854a3a-2127-42	
Repository / Quel Repository					af854a3a-2127-42	

Repository / Oval Repository	a1034a3a-212/-42
git.videolan.org Git - vlc.git/commit	MITRE
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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](#)