CVE-2014-1684

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

Summary

CVE	CVE-2014-1684
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-03-03 16:55:04 UTC
Updated	2026-04-29 01:13:23 UTC
Description	The ASF_ReadObject_file_properties function in modules/demux/asf/libasf.c in the ASF Demuxer in VideoLAN VLC Media

Risk And Classification

Primary CVSS: v2.0 4.3 from nvd@nist.gov

AV:N/AC:M/Au:N/C:N/I:N/A:P

EPSS: 0.127500000 probability, percentile 0.940540000 (date 2026-05-09)

Problem Types: CWE-189 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

AV:N/AC:M/Au:N/C:N/I:N/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	1.1.10	All	All	All
Application	Videolan	Vlc Media Player	1.1.10.1	All	All	All
Application	Videolan	Vlc Media Player	1.1.11	All	All	All
Application	Videolan	Vlc Media Player	1.1.12	All	All	All
Application	Videolan	Vlc Media Player	1.1.13	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	1.1.4.1	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
Application	Videolan	Vlc Media Player	1.1.9	All	All	All
Application	Videolan	Vlc Media Player	2.0.0	All	All	All
Application	Videolan	Vlc Media Player	2.0.1	All	All	All
Application	Videolan	Vlc Media Player	2.0.2	All	All	All
Application	Videolan	Vlc Media Player	2.0.3	All	All	All
Application	Videolan	Vlc Media Player	2.0.4	All	All	All
Application	Videolan	Vlc Media Player	2.0.5	All	All	All
Application	Videolan	Vlc Media Player	2.0.6	All	All	All
Application	Videolan	Vlc Media Player	2.0.7	All	All	All
Application	Videolan	Vlc Media Player	2.0.8	All	All	All
Application	Videolan	Vlc Media Player	2.0.9	All	All	All
Application	Videolan	Vlc Media Player	2.1.0	All	All	All
Application	Videolan	Vlc Media Player	2.1.1	All	All	All

Application	Videolan	Vlc Media Player	2.1.1	All	All	All
Application	Videolan	Vlc Media Player	All	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source	Link
#10482 (Divisoin By Zero DOS POC in VLC 2.1.2 ASF demuer) – VLC	af854a3a-2127-422b-91ae-364da2661108	trac.videolan.org
git.videolan.org Git - vlc.git/commitdiff	af854a3a-2127-422b-91ae-364da2661108	git.videolan.org
VLC ASF Demuxer Division By Zero Bug (CVE-2014-1684) | Saif El-Sherei	af854a3a-2127-422b-91ae-364da2661108	www.elsherei.com
VLC: Multiple vulnerabilities (GLSA 201603-08) — Gentoo Security	af854a3a-2127-422b-91ae-364da2661108	security.gentoo.org
git.videolan.org Git - vlc.git/commitdiff	MITRE	git.videolan.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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 registred 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**