



CVE-2007-6681

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

Summary

CVE	CVE-2007-6681
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-01-17 01:00:00 UTC
Updated	2017-09-29 01:30:00 UTC
Description	Stack-based buffer overflow in modules/demux/subtitle.c in VideoLAN VLC 0.8.6d allows remote attackers to execute arbit

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Videolan	Vlc	All	All	All	All

References

Reference	Source	Link
Debian -- Security Information -- DSA-1543-1 vlc	DEBIAN	www.debian.org
Changelog/0.8.6f - VideoLAN Wiki	CONFIRM	wiki.videolan.org
VLC: Multiple vulnerabilities — Gentoo Linux Documentation	GENTOO	www.gentoo.org
SecurityReason - Buffer-overflow and format string in VideoLAN VLC 0.8.6d	SREASON	securityreason.com
Gentoo update for vlc - Advisories - Secunia	SECUNIA	secunia.com
Gentoo update for vlc - Advisories - Secunia	SECUNIA	secunia.com
Debian update for vlc - Advisories - Secunia	SECUNIA	secunia.com
SecurityFocus	BUGTRAQ	www.securityfocus
alugi.altervista.org/adv/vlcboffs-adv.txt	MISC	alugi.altervista.org
Repository / Oval Repository	OVAL	oval.cisecurity.org
VideoLAN Security Advisory 0801	CONFIRM	www.videolan.org
VideoLAN VLC Multiple Remote Code Execution Vulnerabilities	BID	www.securityfocus
VideoLAN VLC Media Player 0.8.6d SSA Parsing Double Sh311 - Universal - Windows local Exploit	EXPLOIT-DB	www.exploit-db.com

[vlc-devel] vlc: svn commit r20715 (fenrir)	MLIST	mailman.videolan.org
VLC Media Player Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia.com
VLC: User-assisted execution of arbitrary code — Gentoo Linux Documentation	GENTOO	security.gentoo.org
42207	OSVDB	osvdb.org
[vlc-devel] subtitle processing overflows	MLIST	mailman.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 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.

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