CVE-2007-3316

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

Summary

CVE	CVE-2007-3316
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-06-21 18:30:00 UTC
Updated	2018-10-16 16:48:00 UTC
Description	Multiple format string vulnerabilities in plugins in VideoLAN VLC Media Player before 0.8.6c allow remote attackers to cause

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Videolan	Vlc Media Player	0.8.6a	All	All	All
Application	Videolan	Vlc Media Player	0.8.6b	All	All	All
Application	Videolan	Vlc Media Player	0.8.6a	All	All	All
Application	Videolan	Vlc Media Player	0.8.6b	All	All	All

References

Reference	Source	Link	Tags
Repository / Oval Repository	OVAL	oval.cisecurity.org	
37381	OSVDB	osvdb.org	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com	
VLC Media Player Multiple Plugins Format String Vulnerabilities - Advisories - Secunia	SECUNIA	secunia.com	Patch, Vend
Gentoo update for vlc - Advisories - Secunia	SECUNIA	secunia.com	
VLC Media Player Multiple Format String Vulnerabilities	BID	www.securityfocus.com	
SecurityFocus	BUGTRAQ	www.securityfocus.com	
Debian update for vlc - Advisories - Secunia	SECUNIA	secunia.com	
US-CERT Vulnerability Note VU#200928	CERT-VN	www.kb.cert.org	US Governm
www.isecpartners.com/advisories/2007-001-vlc.txt	MISC	www.isecpartners.com	

37380	OSVDB	osvdb.org	
VLC media player: Format string vulnerabilities — Gentoo Linux Documentation	GENTOO	security.gentoo.org	
37382	OSVDB	osvdb.org	
VideoLAN security advisory 0702	CONFIRM	www.videolan.org	Patch
Debian -- Security Information -- DSA-1332-1 vlc	DEBIAN	www.debian.org	
37379	OSVDB	osvdb.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, a

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

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