CVE-2008-4654

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

Summary

CVE	CVE-2008-4654
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-10-22 00:11:00 UTC
Updated	2023-11-07 02:02:00 UTC
Description	Stack-based buffer overflow in the parse_master function in the Ty demux plugin (modules/demux/ty.c) in VLC Media Playe

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Videolan	Vlc Media Player	0.9	All	All	All
Application	Videolan	Vlc Media Player	0.9.1	All	All	All
Application	Videolan	Vlc Media Player	0.9.2	All	All	All
Application	Videolan	Vlc Media Player	0.9.3	All	All	All
Application	Videolan	Vlc Media Player	0.9.4	All	All	All
Application	Videolan	Vlc Media Player	0.9	All	All	All
Application	Videolan	Vlc Media Player	0.9.1	All	All	All
Application	Videolan	Vlc Media Player	0.9.2	All	All	All
Application	Videolan	Vlc Media Player	0.9.3	All	All	All
Application	Videolan	Vlc Media Player	0.9.4	All	All	All

References

Reference	Source
www.trapkit.de/advisories/TKADV2008-010.txt	MISC
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
git.videolan.org Git - vlc.git/commit	CONFIRM
VLC Media Player TY Processing Buffer Overflow Vulnerability - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA

Repository / Oval Repository	OVAL
oss-security - CVE id request: vlc	MLIST
VLC Media Player TY File Stack Based Buffer Overflow Vulnerability	BID
VLC media player TiVo ty Processing Stack Overflow Vulnerability - CXSecurity.com	SREASON
#502726 - vlc: CVE-2008-4654 stack-based buffer overflow in ty parsing - Debian Bug report logs	CONFIRM
git.videolan.org Git - vlc.git/commitdiff	
git.videolan.org Git	
VideoLAN Security Advisory 0809	CONFIRM
git.videolan.org Git - vlc.git/commitdiff	CONFIRM
IBM X-Force Exchange	XF
SecurityFocus	BUGTRAQ
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.