CVE-2007-2498

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

Summary

CVE	CVE-2007-2498
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-05-04 00:19:00 UTC
Updated	2017-10-11 01:32:00 UTC
Description	libmp4v2.dll in Winamp 5.02 through 5.34 allows user-assisted remote attackers to execute arbitrary code via a certain .MP

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nullsoft	Winamp	5.2	All	All	All
Application	Nullsoft	Winamp	5.21	All	All	All
Application	Nullsoft	Winamp	5.22	All	All	All
Application	Nullsoft	Winamp	5.23	All	All	All
Application	Nullsoft	Winamp	5.24	All	All	All
Application	Nullsoft	Winamp	5.3	All	All	All
Application	Nullsoft	Winamp	5.31	All	All	All
Application	Nullsoft	Winamp	5.32	All	All	All
Application	Nullsoft	Winamp	5.33	All	All	All
Application	Nullsoft	Winamp	5.34	All	All	All
Application	Nullsoft	Winamp	5.2	All	All	All
Application	Nullsoft	Winamp	5.21	All	All	All
Application	Nullsoft	Winamp	5.22	All	All	All
Application	Nullsoft	Winamp	5.23	All	All	All
Application	Nullsoft	Winamp	5.24	All	All	All
Application	Nullsoft	Winamp	5.3	All	All	All
Application	Nullsoft	Winamp	5.31	All	All	All

Application	Nullsoft	Winamp	5.32	All	All	All
Application	Nullsoft	Winamp	5.33	All	All	All
Application	Nullsoft	Winamp	5.34	All	All	All

References

Reference	Source	Link
Webmail- OVH	VUPEN	www.vupen.com
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.c
Winamp MP4 File Handling Memory Corruption Vulnerability - Advisories - Secunia	SECUNIA	secunia.com
Winamp MP4 File Parsing Buffer Overflow Vulnerability	BID	www.securityfocus.com
SecurityTracker.com Archives - Winamp MP4 Bug Lets Remote Users Execute Arbitrary Code	SECTRACK	securitytracker.com
Winamp <= 5.34 .MP4 File Code Execution Exploit	EXPLOIT-DB	www.exploit-db.com
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.