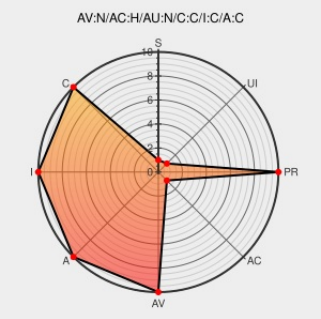
CVE-2005-3188

Published on: 12/31/2005 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:22 PM UTC

CVE-2005-3188

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Winamp from Nullsoft contain the following vulnerability:

Buffer overflow in Nullsoft Winamp 5.094 allows remote attackers to execute arbitrary code via (1) an m3u file containing a long line ending in .wma or (2) a pls file containing a long File1 value ending in .wma, a different vulnerability than CVE-2006-0476.

CVE-2005-3188 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.6 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	HIGH	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
SecurityTracker.com Archives - Winamp Buffer Overflow in Processing '.m3u' File Names May Let Remote Users Execute Arbitrary Code	Vendor Advisory, securitytracker.com, text/html	SECTRACK 1015621
SecurityReason	securityreason.com, text/html	SREASON 397
No Description Provided	Patch, www.osvdb.org, Inactive Link, Not Archived	OSVDB 22975
Advisory: 02.01.06 // VeriSign iDefense	Exploit, Patch, Vendor Advisory, www.idefense.com, text/html	IDEFENSE 20060201 Winamp m3u/pls .WMA Extension Buffer Overflow Vulnerability

SecurityTracker.com Archives - Winamp Error in Processing m3u/pls Files With '.wma' File Extension Lets Remote Users Deny Service	Patch securitytracker.com text/html	SECTRACK 1015565
Nullsoft Winamp Malformed Playlist File WMA Extention Remote Buffer Overflow Vulnerability	cve.report (archive) text/html	BID 16462
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF winamp-wma-ext-bo(24417)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nullsoft	Winamp	5.094	All	All	All
Application	Nullsoft	Winamp	5.094	All	All	All

cpe:2.3:a:nullsoft:winamp:5.094:*:*:*:*:*:*:*:

cpe:2.3:a:nullsoft:winamp:5.094:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→