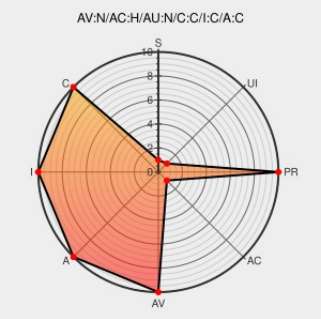
CVE-2004-1896

Published on: 12/31/2004 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:10 PM UTC

CVE-2004-1896

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



Certain versions of Winamp from Nullsoft contain the following vulnerability:

Heap-based buffer overflow in in_mod.dll in Nullsoft Winamp 2.91 through 5.02 allows remote attackers to execute arbitrary code via a Fasttracker 2 (.xm) mod media file.

CVE-2004-1896 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
Winamp Fasttracker 2 File 'in_mod.dll' Heap Overflow Lets Remote Users Execute Arbitrary Code - SecurityTracker	securitytracker.com text/html	SECTRACK 1009660
nextgenss.com - This website is for sale! - nextgenss Resources and Information.	Patch www.nextgenss.com text/plain	MISC www.nextgenss.com/advisories/winampheap.txt
'NGSSoftware Insight Security Research Advisory' - MARC	marc.info text/html	BUGTRAQ 20040405 NGSSoftware Insight Security Research Advisory
Secunia - Advisories - Winamp "in_mod.dll" Heap Overflow Vulnerability	Patch web.archive.org text/html	SECUNIA 11285
NullSoft Winamp in_mod.dll Plug-in Heap Overflow Vulnerability	Patch cve.report (archive) text/html	BID 10045

No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 4944
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF winamp-inmod-bo(15727)

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	2.91	All	All	All
Application	Nullsoft	Winamp	3.0	All	All	All
Application	Nullsoft	Winamp	3.1	All	All	All
Application	Nullsoft	Winamp	5.0.1	All	All	All
Application	Nullsoft	Winamp	5.0.2	All	All	All
Application	Nullsoft	Winamp	2.91	All	All	All
Application	Nullsoft	Winamp	3.0	All	All	All
Application	Nullsoft	Winamp	3.1	All	All	All
Application	Nullsoft	Winamp	5.0.1	All	All	All
Application	Nullsoft	Winamp	5.0.2	All	All	All

cpe:2.3:a:nullsoft:winamp:2.91:*:*:*:*:*:*:*:

cpe:2.3:a:nullsoft:winamp:3.0:*:*:*:*:*:*:*:

cpe:2.3:a:nullsoft:winamp:3.1:*:*:*:*:*:*:*:

cpe:2.3:a:nullsoft:winamp:5.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:nullsoft:winamp:5.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:nullsoft:winamp:2.91:*:*:*:*:*:*:*:

cpe:2.3:a:nullsoft:winamp:3.0:*:*:*:*:*:*:*:

cpe:2.3:a:nullsoft:winamp:3.1:*:*:*:*:*:*:*:

cpe:2.3:a:nullsoft:winamp:5.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:nullsoft:winamp:5.0.2:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→