



CVE-2005-2310

Published on: 07/19/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:28 PM UTC

CVE-2005-2310

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Winamp](#) from [Nullsoft](#) contain the following vulnerability:

Buffer overflow in Winamp 5.03a, 5.09 and 5.091, and other versions before 5.094, allows remote attackers to execute arbitrary code via an MP3 file with a long ID3v2 tag such as (1) ARTIST or (2) TITLE.

CVE-2005-2310 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **9.3 - HIGH**

Access
Vector

NETWORK

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

No Description Provided

www.osvdb.org

[OSVDB 17897](#)

Inactive Link Not Archived

404 Not Found

Exploit

Vendor Advisory

web.archive.org

text/html

Inactive Link Not Archived

[MISC security.lss.hr/index.php?page=details&ID=LSS-2005-07-14](http://MISC.security.lss.hr/index.php?page=details&ID=LSS-2005-07-14)

Secunia - Advisories - Winamp ID3v2 Tag Handling Buffer Overflow Vulnerability

Vendor Advisory

web.archive.org

text/html

[SECUNIA 16077](#)

SecurityTracker.com Archives - Winamp MP3 ID3v2 Tag Buffer Overflow Lets Remote Users Execute Arbitrary Code

Exploit

securitytracker.com

text/html

[SECTRAK 1014483](#)

Nullsoft Winamp Malformed ID3v2 Tag Buffer Overflow Vulnerability	cve.report (archive) text/html	 BID 14276
Winamp Media Player » Player » Version History	web.archive.org text/html Inactive Link Not Archived	 CONFIRM www.winamp.com/player/version_history.php
Webmail - OVH	www.vupen.com text/html	 VUPEN ADV-2005-1106

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	5.03a	All	All	All
Application	Nullsoft	Winamp	5.09	All	All	All
Application	Nullsoft	Winamp	5.091	All	All	All
Application	Nullsoft	Winamp	5.03a	All	All	All
Application	Nullsoft	Winamp	5.09	All	All	All
Application	Nullsoft	Winamp	5.091	All	All	All
Application	Nullsoft	Winamp	All	All	All	All
cpe:2.3:a:nullsoft:winamp:5.03a:*:*:*:*:*:						
cpe:2.3:a:nullsoft:winamp:5.09:*:*:*:*:*:						
cpe:2.3:a:nullsoft:winamp:5.091:*:*:*:*:*:						
cpe:2.3:a:nullsoft:winamp:5.03a:*:*:*:*:*:						
cpe:2.3:a:nullsoft:winamp:5.09:*:*:*:*:*:						
cpe:2.3:a:nullsoft:winamp:5.091:*:*:*:*:*:						
cpe:2.3:a:nullsoft:winamp:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)