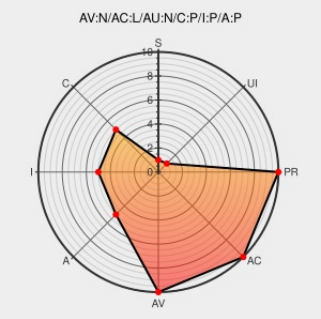
CVE-2008-3441

Published on: 08/01/2008 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:11 PM UTC

CVE-2008-3441

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



Certain versions of Winamp from Nullsoft contain the following vulnerability:

Nullsoft Winamp before 5.24 does not properly verify the authenticity of updates, which allows man-in-the-middle attackers to execute arbitrary code via a Trojan horse update, as demonstrated by evilgrade and DNS cache poisoning.

CVE-2008-3441 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
	Third Party Advisory, www.infobyte.com.ar, application/gzip, Inactive Link, Not Archived	MISC www.infobyte.com.ar/down/isr-evilgrade-1.0.0.tar.gz
Repository / Oval Repository	Third Party Advisory, oval.cisecurity.org, text/html	OVAL oval:org.mitre.oval:def:15225
	Third Party Advisory, www.infobyte.com.ar, application/pdf, Inactive Link, Not Archived	MISC www.infobyte.com.ar/down/Francisco%20Amato%20-%20evilgrade%20-%20ENG.pdf
No Description Provided	Broken Link, web.archive.org, text/html	FULLDISC 20080728 Tool release: [evilgrade] - Using DNS cache poisoning to exploit poor update implementations

	Inactive Link Not Archived	
Winamp Update Component Lack of Digital Signatures Lets Remote Users Install Arbitrary Code in Certain Cases - SecurityTracker	Third Party Advisory VDB Entry securitytracker.com text/html	SECTRACK 1020582

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	All	All	All	All
Application	Nullsoft	Winamp	All	All	All	All

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report