

[NT] Buffer Overflow in WinAMP in_cdda.dll CDA Device Name

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-01/0128.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 01/27/05

To: list@securiteam.com

Date: 27 Jan 2005 18:43:34 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Buffer Overflow in WinAMP in_cdda.dll CDA Device Name

SUMMARY

WinAMP is "a popular media player that supports various media and playlist formats, including playlists in m3u or pls format".

NSFocus Security Team has found a buffer overflow vulnerability in the plug-in by which WinAMP plays CD. An attacker can construct a malicious playlist file that is embedded in a HTML page. If a user is persuaded to click it, then the attacker can gain complete control over the user's system.

DETAILS

Vulnerable Systems:

- * Nullsoft WinAMP version 5.08 and prior

Immune Systems:

- * Nullsoft WinAMP version 2.xx
- * Nullsoft WinAMP version 5.08c or newer

WinAMP implements various functionalities through different plug-ins that

Securiteam: [NT] Buffer Overflow in WinAMP in_cdda.dll CDA Device Name

are stored in "plugins" sub-directory of WinAMP installation directory. For example, in_mp3.dll is used to play MP3 files and in_cdda.dll is used to play CD.

The in_cdda.dll of WinAMP supports play path requests in the following format:

1. <Driver><PathName>[FileName].cda
2. linein://
3. cda://
4. cda://<Driver>
5. cda://<Driver>,<TrackNumber>

Brett Moore of Security-Assessment.com discovered a stack overflow when in_cdda.dll handles the first path. WinAMP released version 5.07 to fix that vulnerability.

Actually, in_cdda.dll will still cause an overflow when handling 4th and 5th path above. Stack overflow will be triggered only by adding an over-long device name or sound track number behind "cda://".

Any method that can pass a play path to WinAMP can be used to trigger this vulnerability, for example, command line.

One possible remote attacking vector is to construct a playlist file in m3u or pls format with an over-long path embedded in HTML. Once a user visits such a malicious page, it will execute the code of attacker's choice.

Workaround:

NSFOCUS suggests to remove in_cdda.dll from Plugins of WinAMP.

Vendor Status:

2004.11.24 – Informed the vendor support@winamp.com, no response

2004.12.06 – Tests proved WinAMP 5.07 is affected, informed the vendor again

2004.12.07 – The vendor confirmed the vulnerability

2004.12.25 – Tests proved WinAMP 5.08 is affected, informed the vendor

2005.01.10 – The vendor released WinAMP 5.08c to fix the vulnerability

The vendor has released WinAMP 5.08c to fix this vulnerability. The latest version is available at <<http://www.winamp.com/player/>>
<http://www.winamp.com/player/>

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1150>>
CAN-2004-1150

ADDITIONAL INFORMATION

The information has been provided by <mailto:security@nsfocus.com>
NSFOCUS Security Team.

Securiteam: [NT] Buffer Overflow in WinAMP in_cdda.dll CDA Device Name

The original article can be found at:

<<http://www.nsfocus.com/english/homepage/research/0501.htm>>

<http://www.nsfocus.com/english/homepage/research/0501.htm>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.