

[NT] MP3 Files can Cause Code Execution under Winamp

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-04/0119.html>

From: support@securiteam.com

Date: 04/29/02

From: support@securiteam.com

To: list@securiteam.com

Date: Mon, 29 Apr 2002 09:19:42 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

MP3 Files can Cause Code Execution under Winamp

SUMMARY

It is possible to modify an existing MP3 file in such a way that it can carry a virus. The virus is activated when the MP3 file is played in Winamp and can then infect other MP3 files found on hard drives or network shares. In order to protect yourself you need to upgrade to Winamp 2.80 or disable the minibrowser.

DETAILS

Vulnerable systems:

Nullsoft Winamp version 2.79

Immune systems:

Nullsoft Winamp version 2.80

An MP3 file can contain the ID3v2 tag. It is a newer version of the ID3v1 tag and carries information like title, artist, and album. The tag is parsed by Winamp when an MP3 file is loaded.

If the minibrowser is enabled, Winamp will try to query a script on <http://info.winamp.com> for extra information about the song, based on data

Securiteam: [NT] MP3 Files can Cause Code Execution under Winamp

Once we control the EIP, we have to do something useful. Since we still are limited in what kind of op-codes we can construct, it's better to try to get somewhere in memory where our URL is not escaped (ex. ! to %21). When debugging we notice the register ECX is 0x12bd00 and points to a copy of our URL partly un-escaped. Therefore, if we somehow can increase the ECX and change the memory to do JMP ECX we are on a address where we can create any op-code we want. This can be done with op-codes like:
0x66335142 ("f3QB") XOR DX,[ECX+0x42]
0x4A ("J") DEC EDX
0x665A ("fZ") POP DX
0x6652 ("fR") PUSH DX

It is not an easy task to perform the above and on some OS, it has to be done differently, but still it is possible.

ADDITIONAL INFORMATION

The information has been provided by <mailto:sandblad@acc.umu.se> Andreas Sandblad.

=====

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.

-
- **Previous message:** support@securiteam.com: "[UNIX] PHP-Survey Global.INC Information Disclosure Vulnerability"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)