

[NT] Winamp ID3v2 Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-07/0044.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 07/18/05

To: list@securiteam.com

Date: 18 Jul 2005 19:07:41 +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>

Winamp ID3v2 Buffer Overflow

SUMMARY

<<http://www.winamp.com/>> Winamp is "a skinnable, multi-format, freeware audio player made by Nullsoft".

The vulnerability discovered in Winamp's ID3v2 could be used to spread malicious code such as a virus within MP3 files, which are commonly very trusted.

DETAILS

Vulnerable Systems:

- * Winamp version 5.03a
- * Winamp version 5.09
- * Winamp version 5.091

Winamp is vulnerable to a buffer overflow vulnerability when processing ID3v2 tags of mp3 files. To exploit this vulnerability, a user has to add malformed mp3 file to the Winamp playlist, and play it. When playing mp3 file is finished, playlist is updated, and if some part of the ID3v2 tag (e.g. ARTIST or TITLE) is too long, it is possible to overflow value that is later used as the source address in the strcpy() function. The strcpy() call can overflow a value (in the DATA segment) that will later, in jump

Securiteam: [NT] Winamp ID3v2 Buffer Overflow

instruction, point code execution to some attacker-supplied buffer, where malicious code can be executed.

Before it is possible to overflow important value in the DATA segment, a simple "sanity check" has to be passed. In the next piece of asm code, we control the EAX register (because of the first overflow), and after returning from the function, that EAX is used as source address for strcpy().

This "sanity check" code will test if there is a value 0x00000001 (ECX) in memory on offset 0x9B4 from EAX address. If that condition is true, then after returning from the function, the same EAX content will be used as the source address in strcpy(). If the condition is false, EAX is set to a value that is located on offset 0x9B8 from current EAX register address, and the program will jump to the beginning of the loop.

```
-----004371FA /$
8B4424 04 MOV EAX,DWORD PTR SS:[ESP+4]004371FE |> 85C0
/TEST EAX,EAX00437200 |. 74 14 |JE SHORT Winamp.0043721600437202
|. 8B88 B4090000 |MOV ECX,DWORD PTR DS:[EAX+9B4]00437208 |. 3B4C24 08
|CMP ECX,DWORD PTR SS:[ESP+8]0043720C |. 74 0D |JE SHORT
Winamp.0043721B0043720E |. 8B80 B8090000 |MOV EAX,DWORD PTR
DS:[EAX+9B8]00437214 |.^EB E8 \JMP SHORT Winamp.004371FE00437216
|> B8 DC124600 MOV EAX,Winamp.004612DC ; ASCII "No Entry"0043721B
\> C3
RETN-----
```

Here is that asm code roughly reversed:

```
char *check (char *arg, int val) // val = 0x00000001
{
    while (arg != NULL)
    {
        if (*(int*)&arg[2484] == val) // 0x9b4 = dec. 2484
            return arg;
        else arg = (char*)((long*)&arg[2488]); // 0x9b8 = dec. 2488
    }
    arg = "No Entry";
    return arg;
}
```

To bypass that check, EAX (arg) has to be set to the address of string buffer where on address EAX+9B4 is value 0x00000001 (val), and that string has to be still long enough to overflow onto the "jump address". The string needs to be at least 284 bytes long to overflow onto the "jump address" in the DATA segment. The ID3v2 data resides in the DATA segment (that is static), and there are a lot of 0x00000001 values in it, so it is possible to determine a static address that will work every time for some Winamp and Windows versions.

Due to the fact that if condition EAX+9B4=0x00000001 isn't met, EAX is set to value at address EAX+9B8 and condition would be tested again, maybe it is even possible to create some brute-force buffer(s) that will "scan" the

Securiteam: [NT] Winamp ID3v2 Buffer Overflow

memory for 0x00000001, but this is purely theoretical, and probably unlikely.

When the "sanity check" is bypassed, strcpy() will be executed, and the "jump address" will be overflowed. That strcpy() code is presented below.

```
-----00438D59 |. 50
    PUSH EAX ; /src = "FFFFFFFFFFFFFFFFFFFFF..."00438D5A |. FF75
08 PUSH DWORD PTR SS:[EBP+8] ; |dest00438D5D |. E8 60D20100
    CALL <JMP.&MSVCRT strcpy> ;
\strcpy-----
```

The destination address for strcpy() is 280 bytes away from the "jump address" that has to be overflowed to redirect code execution. In this particular example, it is 0x00470D40.

After that is done, next piece of code will take the overflowed "jump address" from address 0x00470E58 and point code execution onto it.

```
-----0041D440 /$ A1
580E4700 MOV EAX,DWORD PTR DS:[470E58]0041D445 |. 85C0 TEST
EAX,EAX0041D447 |. 74 03 JE SHORT winamp.0041D44C0041D449 |.
FF60 48 JMP DWORD PTR DS:[EAX+48] <- 0wnZ Winamp0041D44C \> C3
    RETN-----
```

Its possible to reliably exploit this vulnerability on Windows XP SP1 and windows 2000 SP0, with Winamp versions 5.03a, 5.09 and 5.091.

It is important to say that this vulnerability is not easy to exploit, but with the help of static addresses from the DATA segment, it is possible to create reliable exploit. Beside, there are few possible exploitation vectors for this vulnerability, depending on what actions are performed by user on malformed mp3 file. For example – in version 5.03a, if the malformed mp3 file is added to the playlist with 'add-folder' option, it isn't needed to bypass the previously mentioned "sanity check".

Proof of concept:

<<http://security.lss.hr/PoC/demo.mp3>> <http://security.lss.hr/PoC/demo.mp3>

ADDITIONAL INFORMATION

The original article can be found at:

<<http://security.lss.hr/index.php?page=details&ID=LSS-2005-07-14>>

<http://security.lss.hr/index.php?page=details&ID=LSS-2005-07-14>

The information has been provided by <mailto:ljuranic@lss.hr> Leon Juranic.

=====

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

Securiteam: [NT] Winamp ID3v2 Buffer Overflow

=====
=====

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.