

[NT] AOL Nullsoft Winamp IT Module Heap Memory Corruption (IN_MOD.DLL)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-04/msg00018.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 8 Apr 2007 13:14:19 +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>

AOL Nullsoft Winamp IT Module Heap Memory Corruption (IN_MOD.DLL)

SUMMARY

<<http://www.winamp.com/>> Winamp is "a proprietary media player written by Nullsoft, a subsidiary of Time Warner. It is skinnable, multi-format freeware / shareware". Successful exploitation may allow the attacker to run arbitrary code in context of user running AOL Nullsoft Winamp.

DETAILS

Vulnerable Systems:

* AOL Nullsoft Winamp version 5.33 (x86) Feb 13 2007 (on Windows XP SP1/SP2).

The problem takes place when Winamp is trying to play specially crafted IT file.

IT is the proprietary module format used by Impulse Tracker, featuring support for more advanced features than MOD or S3M before it. These include a larger limit for lines in a pattern, higher quality samples, and other effects.

[NT] AOL Nullsoft Winamp IT Module Heap Memory Corruption (IN_MOD.DLL)

Take a look at this code snippet:

```
-----// SNIP SNIP //-----  
text:00E97BCA write_looop: ; CODE XREF:  
sub_E97976+29D#j  
text:00E97BCA mov edx, [ebp+6Ch+arg_0]  
text:00E97BCD mov ecx, [ebx+18h]  
text:00E97BD0 mov dx, [eax+edx*2]  
text:00E97BD4 mov [eax+ecx*2], dx  
text:00E97BD8 mov eax, [ebx+370h]  
text:00E97BDE mov ecx, [ebx+18h]  
text:00E97BE1 mov cx, [eax+ecx*2]  
text:00E97BE5 cmp cx, [esi+6Eh]  
text:00E97BE9 jnb short loc_E97C09  
text:00E97BEB mov al, [ebx+18h]  
text:00E97BEE mov ecx, [ebp+6Ch+arg_0]  
text:00E97BF1 mov [ecx+esi+148h], al ; BANG  
text:00E97BF8 mov eax, [ebx+370h]  
text:00E97BFE cmp word ptr [eax+ecx*2], 0FEh  
text:00E97C04 jnb short loc_E97C09  
text:00E97C06 inc dword ptr [ebx+18h]  
text:00E97C09  
text:00E97C09 loc_E97C09: ; CODE XREF:  
sub_E97976+273#j  
text:00E97C09 ; sub_E97976+28E#j  
text:00E97C09 movzx ecx, word ptr [esi+68h] ;  
ecx=controlled value (from offset 0x20)  
text:00E97C0D inc [ebp+6Ch+arg_0]  
text:00E97C10 cmp [ebp+6Ch+arg_0], ecx  
text:00E97C13 jb short write_looop  
-----// SNIP SNIP //-----
```

The memory is overwritten at 0x00E97BF1. The description of this disassembly listing is pretty similar to the one written in s3m module files advisory.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:bania.piotr@xxxxxxxxx>> Piotr Bania.

The original article can be found at:

<http://www.piotrbania.com/all/adv/nullsoft-winamp-it_module-in_mod-adv.txt>
http://www.piotrbania.com/all/adv/nullsoft-winamp-it_module-in_mod-adv.txt

=====

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

[NT] AOL Nullsoft Winamp IT Module Heap Memory Corruption (IN_MOD.DLL)

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

list-unsubscribe@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====
=====

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.