Sign in

wildptr-io / **Winrar-CVE-2023-40477-POC**

Public

Notifications   Fork 9   Star 25

Code   Issues   Pull requests   Actions   Projects   Security   Insights

main

Go to file   Code

example_poc_after_gen

README.md

cve_2023_40477_poc...

About

CVE-2023-40477 PoC by Wild-Pointer

Readme

Activity

Custom properties

25 stars

0 watching

9 forks

Report repository

Releases

No releases published

Packages

No packages published

Languages

● **Python** 100.0%

README

CVE-2023-4047 PoC By Wild Pointer

- Read Research: https://wildptr.io/winrar-cve-2023-40477-poc-new-vulnerability-winrar-security-research/
- Recvol3.cpp Vulnerability: https://www.rarlab.com/vuln_rev3_names.html, https://www.win-rar.com/
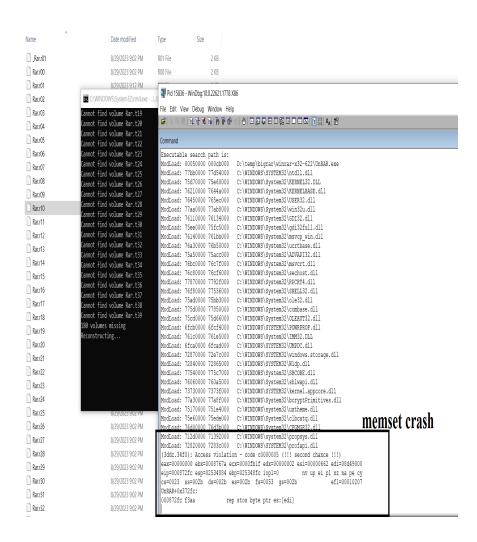- Vulnerable: WinRAR <= 6.22

How to Test?

You can generate your own PoC OR just test attached demo RAR file (verified to crash winrar-6.22 upon extraction).
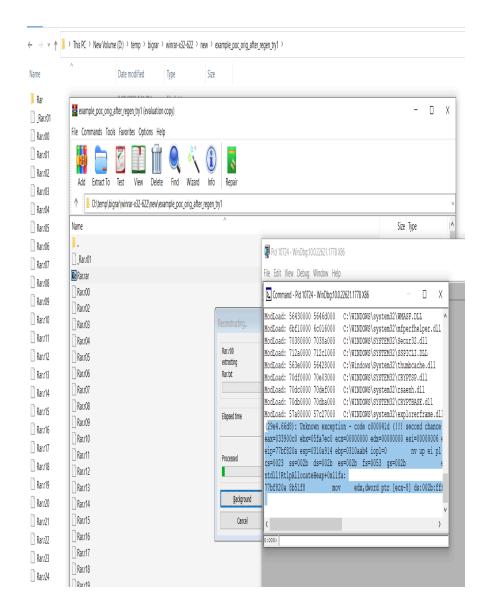
1. PoC Generate - follow `cve_2023_40477_poc.py`
2. Demo RAR file - Just extract `Rar.rar` from `example_poc_after_gen` .

PoC Crash Images

1. Memset Crash-

memset crash

2. Heap Overflow in Winrar -

DISCLAIMER

Use at your own responsibility - The publisher, author or any of its affiliates aren't responsible for any actions caused, made or generated by using this code and/or repository. This is just & solely for educational purposes and includes demo example only, not to harm or cause any impact. Use this for educational purposes only. Do not use this piece of code for any unethical

Terms   Privacy   Security   Status   Docs   Contact   Manage cookies   Do not share my personal information