Product Solutions Resources Open Source Enterprise Pricing Sign in Sign up

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

barakolo Add files via upload a11ef13 · last year 10 Commits

example_poc_after_gen	Add files via upload	last year
README.md	Update README.md	last year
cve_2023_40477_poc.py	Create cve_2023_40477_poc.py	last year

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-

About

CVE-2023-40477 PoC by Wild-Pointer

Readme
Activity
Custom properties
25 stars
0 watching
9 forks
Report repository

Releases

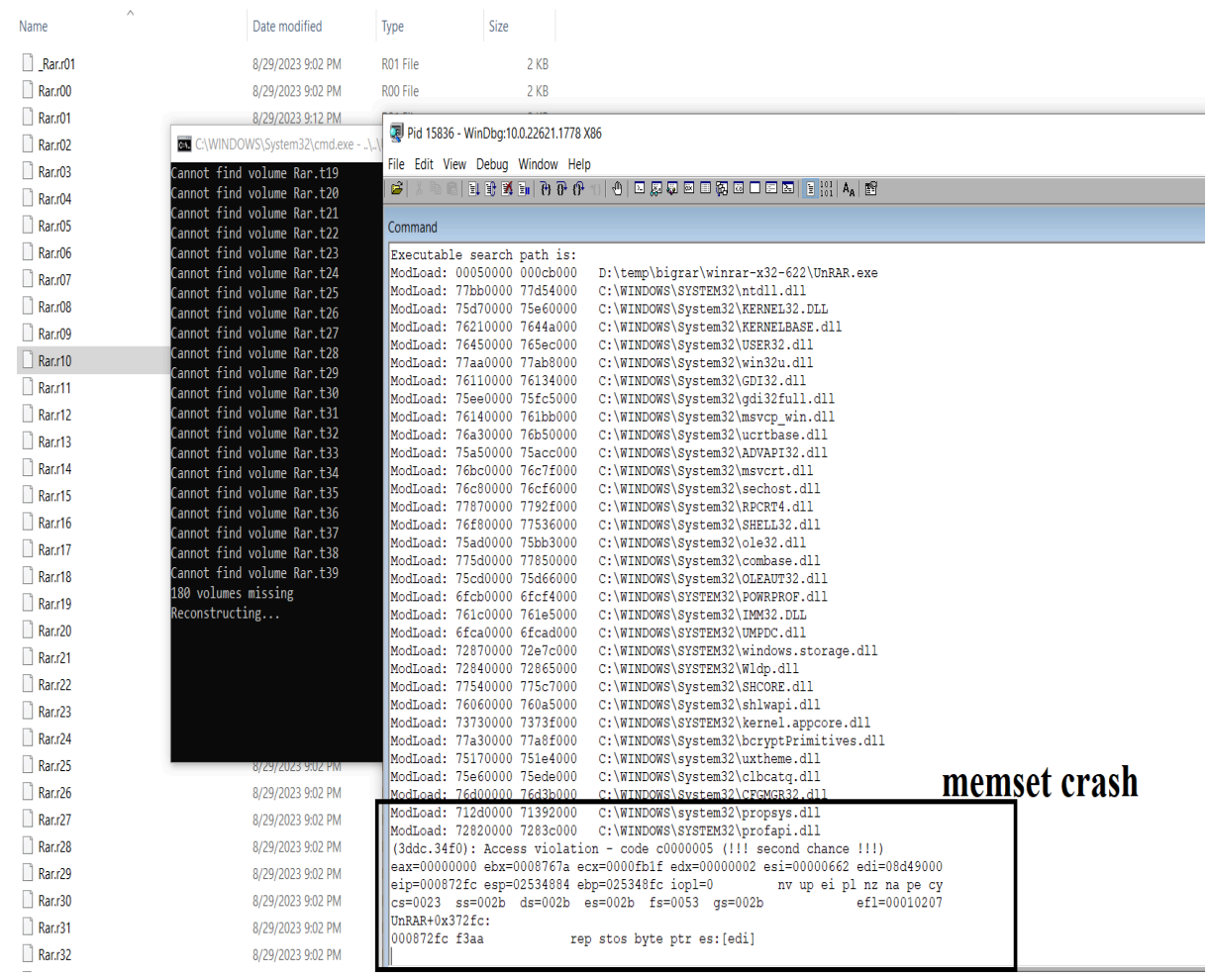
No releases published

Packages

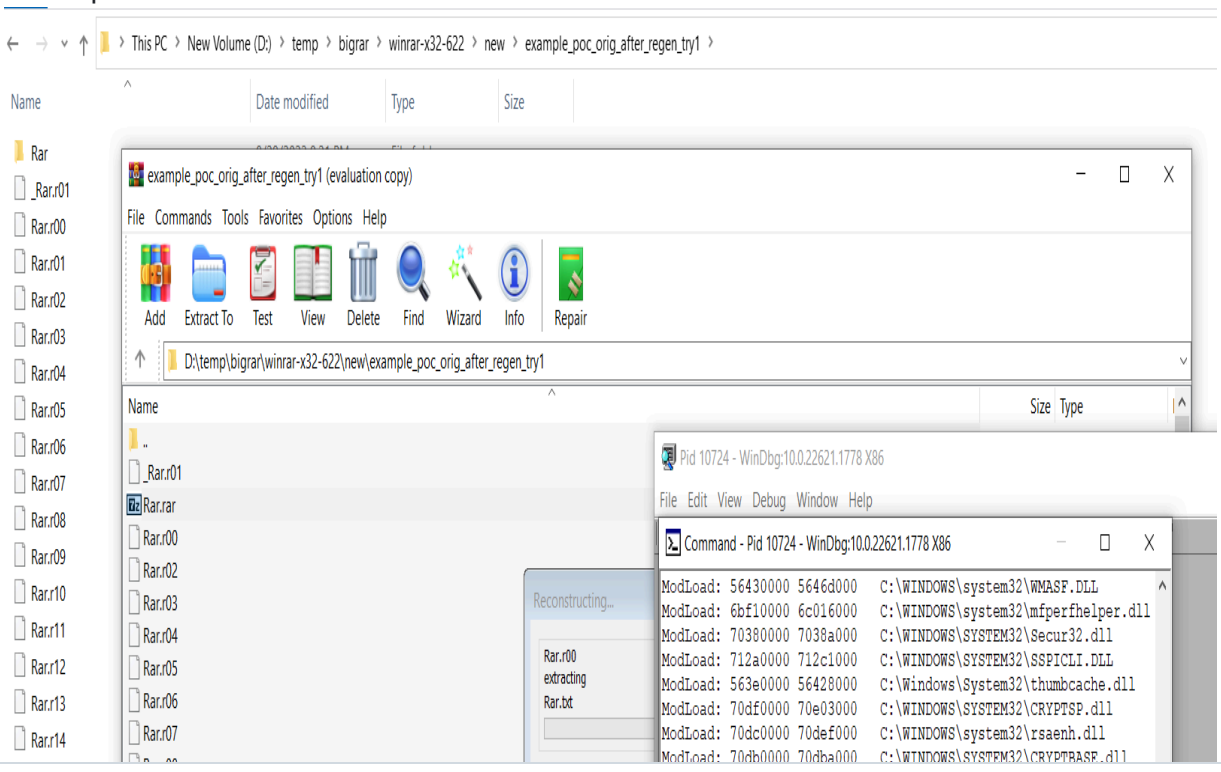
No packages published

Languages

Python 100.0%



2. Heap Overflow in Winrar -



© 2024 GitHub, Inc. Terms Privacy Security Status Docs Contact Manage cookies Do not share my personal information