Privilege Escalation Vulnerability Report

CVE ID: CVE-2021-4034

Vulnerability Name: PwnKit - Polkit pkexec Local Privilege Escalation

Discovered By: Qualys Research Team

Published Date: January 25, 2022

CVSS Score: 7.8 (High)

Affected Systems: Most Linux distributions

Overview:

CVE-2021-4034 is a vulnerability in the pkexec command of Polkit, a component used in many Linux distributions to control system-wide privileges. Due to improper input validation, attackers can exploit it to gain root privileges from an unprivileged account.

How It Was Performed:

- The vulnerability exists in the way pkexec handles command-line arguments.
- If a user runs pkexec without any arguments, it tries to access a non-existent memory region.
- By crafting a malicious environment (especially using GCONV_PATH), an attacker can exploit this and execute arbitrary code as root.

Impact:

- Local privilege escalation: Any unprivileged local user can gain root access.
- Full system compromise in shared environments like servers, cloud containers, etc.

Remediation Plan:

1. Patch/Update:
   - Apply patches provided by your Linux distribution. Example:

```
sudo apt update && sudo apt upgrade polkit
```

2. Temporary Mitigation:
   - Remove the setuid bit from pkexec:

```
chmod 0755 /usr/bin/pkexec
```

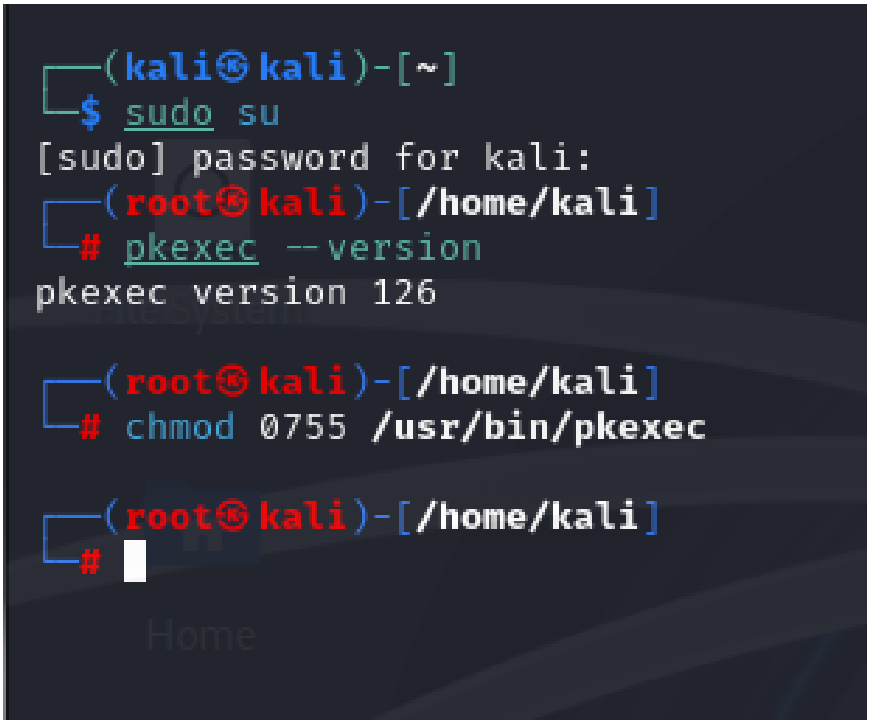
3. Monitoring:
   - Watch for unusual pkexec usage or GCONV_PATH changes.

Conclusion:

CVE-2021-4034 (PwnKit) is a straightforward yet powerful privilege escalation vulnerability affecting Linux systems. It's a perfect example of how small coding mistakes (like uninitialized pointers) can lead to severe security issues. Keeping systems updated and performing regular vulnerability assessments are key to prevention.

Screenshot: Verification and Mitigation

The following screenshot shows the verification of the vulnerable pkexec version and the application of a mitigation step by removing the setuid bit using chmod 0755:



```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# pkexec --version
pkexec version 126

┌──(root㉿kali)-[/home/kali]
└─# chmod 0755 /usr/bin/pkexec

┌──(root㉿kali)-[/home/kali]
└─# 
```