Polkit Privilege Escalation Vulnerability

CVE-ID:

CVE-2021-4034

CVSS-SCORE: 7.8

ATTACK VECTOR: LOCAL

POLKIT(PolicyKit):

A toolkit for controlling system-wide privileges in linux OS, provides a mechanism for non-privileged processes to communicate with privileged processes. Mainly handle authorization.
By the help of “pkexec” command utility

PKEXEC:

Command utility in “polkit”
alternative of “sudo” command
use to execute command with elevated privilege
allow unauthorized user to execute command as another user, if username is not specified then command run as “root” user [THIS IS THE MAJOR CAUSE OF VULNERABILITY]
If PROGRAM is not specified, the default shell will be run.

PWNKIT:

Memory corruption bug for local privilege escalation.

It is exploitable even if the polkit daemon itself is not running.
Any unprivileged local user can exploit this vulnerability to obtain full root privileges.

EXPLOIT:

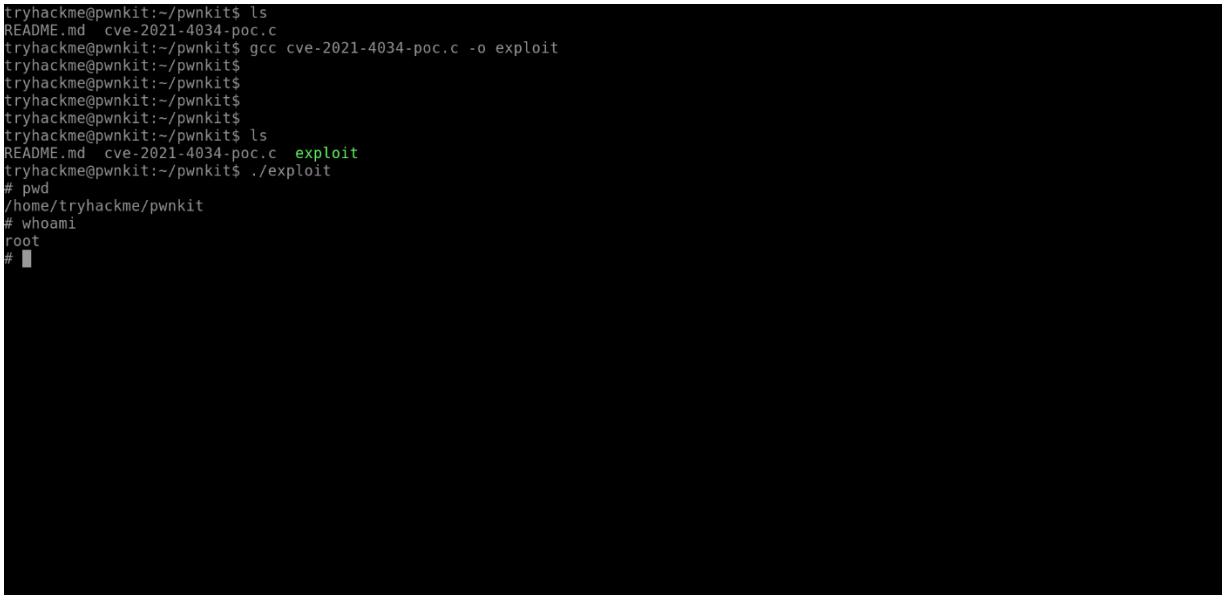
https://github.com/berdav/CVE-2021-4034/blob/main/cve-2021-4034.c
Use this script if your want to automate:

Polkit Privilege Escalation Vulnerability

https://raw.githubusercontent.com/berdav/CVE-2021-4034/main/cve-2021-4034.sh

To check system is exploitable or not you can use this script:
https://access.redhat.com/sites/default/files/cve-2021-4034--2022-01-25-0936.sh

POC:



MITIGATION:

Common mitigation for all linux OS:

1) Update OS
2) Remove the SUID-bit from pkexec as a temporary mitigation: “chmod 0755 usr/bin/pkexec”

FOR RED HAT:

- Install polkit debug info:
  - `debuginfo-install polkit`
- Create the following systemtap script, and name it pkexec-block.stp:

Polkit Privilege Escalation Vulnerability

```
probe process("/usr/bin/pkexec").function("main") {
if (cmdline_arg(1) == "")
raise(9);
}
```

- Load the systemtap module into the running kernel:
  - `stap -g -F -m stap_pkexec_block pkexec-block.stp`
- Ensure the module is loaded:
  - `lsmod | grep -i stap_pkexec_block`
  - `stap_pkexec_block 434176 0`
- After polkit package updated then remove this systemtap script:
  - `rmmod stap_pkexec_block`

[Note] If the system is rebooted, the module generated by the systemtap needs to be reloaded into the kernel. To do that again. Mainly 4th and 5th step.

LAB:

https://tryhackme.com/room/pwnkit