CVE-2021-4034 - Faille dans le paquet polkit (non installé par défaut) (2022)

Sommaire

Description

En préambule, cette faille n'impacte pas directement notre processus d'installation de Shinken, mais suivant l'image d'origine Centos / Redhat, ou suivant les packages qui ont été installés, cette page vous permettra de contourner le problème en attendant le fix officiel.

Les détails de la faille dans la commande polkit sont dans https://blog.qualys.com/vulnerabilities-threat-research/2022/01/25/pwnkit-local-privilege-escalation-vulnerability-discovered-in-polkits-pkexec-cve-2021-4034

En résumé:

- On peux avoir un passage root d'un utilisateur (*genre shinken*) si et seulement si, un utilisateur arrive à lancer la commande **polkit**.

Pour détecter que l'on est vulnérable

```
$ rpm -qa | grep polkit
```

Retour	Vulnérable (ou pas)
non installé	FIXE
installé, version polkit-0.112-26 et inférieure	VULNERABLE
installé, version polkit-0.112-26_**1** et supérieure	FIXE

Impact et correction de la faille

- Dans le cadre de Shinken Enterprise, nous n'installons **PAS** la commande **polkit**.
- Ainsi, la seule possibilité de l'avoir est d'avoir installé un outil tiers qui lui en a besoin
- A ce jour (27 janvier 2022), **la correction consiste à enlever le bit suid du binaire polkit**:
    - `chmod 0755 /usr/bin/pkexec`
- Pour ceux qui sont en système RedHat, un paquet est déjà disponible qui corrige le problème:
    - `yum install -y polkit`

IMPORTANT: Centos6 n'est PAS fixé

Remarque: en Centos6, vu que le système n'est plus supporté, il n'y a pas de correction, il FAUT passer ses serveurs en Centos7