[Privesc/Linux] Looney Tunables

Introduction

Cette faille de type **buffer overflow**, a été trouvée en septembre 2023 dans la **lib_c**.

Elle permet une **escalade de privilège** sur la majorité des distributions Linux.

Exploitation

- Depuis le shell de votre utilisateur standard, cloner le dépôt github :

```
git clone https://github.com/lrustand/CVE-2023-4911
```

- Compiler :

```
make
```

- Et lancer l'exploit :

```
./exploit
```

Selon votre chance vous pouvez attendre quelques secondes à quelques minutes avant de voir apparaître un shell root si l'exploit a fonctionné.

Revision #5
Created 10 October 2023 14:19:25 by Elieroc
Updated 3 May 2024 13:31:00 by Elieroc