Pourquoi? Cible très large

Distributions affectées

- liblzma est utilisée par une version patchée d'OpenSSH pour **systemd**
  - Pas un problème dans OpenSSH upstream
  - Pas un problème pour les distributions n'utilisant pas systemd
- Distribution **rolling-release** basée sur Debian et RedHat sont affectées
  - Debian unstable, Ubuntu Noble, Fedora, Kali, …
    - Toutes ont rollback xz-utils depuis
  - N/A: Debian stable, RHEL, Gentoo

Démo

Cryptographie dans la backdoor

- La backdoor contient une clé publique ED448

```
0a 31 fd 3b 2f 1f c6 92 92 68 32 52 c8 c1 ac 28
34 d1 f2 c9 75 c4 76 5e b1 f6 88 58 88 93 3e 48
10 0c b0 6c 3a be 14 ee 89 55 d2 45 00 c7 7f 6e
20 d3 2c 60 2b 2c 6d 31 00
```

- Les 32 premiers bytes servent à déchiffrer la commande avec ChaCha20
  - Probablement pour éviter la détection
- La clé complète sert à vérifier une signature RFC-8032 ED448
  - Afin d’authentifier l’attaquant