Qui? XZ-Utils

Projet open source largement distribué

- Outils en ligne de commande
  - Similaire à gzip, bzip2
  - xz, unxz, xzcat, xzgrep, …
  - Format de fichier .xz
- Librairie de compression compromise: **liblzma**
  - Utilisée (entre autre) par systemd-notify
  - Patched par-dessus OpenSSH par les distributions utilisant systemd

Quand? Le mois passé

Publication rapide, avant d’atteindre les canaux stables

- 23 Février 2024: code malicieux ajouté à xz-utils
- 24 Février 2024: xz-5.6.0.tar.gz publiée avec la backdoor
- 28 Mars 2024: Andres Freund (Postgres dev chez Microsoft)
  - Enquête sur régression de performances de ses serveurs
  - Réalise la présence d’une backdoor
  - Notifie Debian et Openwall en privé
  - RedHat assigne **CVE-2024-3094** avec **CVSS** de **10**
- 29 Mars 2024: publication sur Openwall “oss-security”