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”

Quoi? Remote Code Execution

Compromission de serveur OpenSSH

- Démarrage du serveur sshd
  - Chargement de systemd-notify, et donc liblzma
  - Mise en place du **trigger** avant RSA_public_decrypt
- Lors du login d’un client via ssh
  - Check la requête du client pour une commande chiffrée
  - Exécute la commande as **root**, contournant l’authentification