

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

Comment? Hidden in plain sight

Publiée sur le dépôt git dans les fichiers tests

- PR merged par Jia Tan, un **maintainer** de XZ
 - Fichier malicieux **obfusqué**: tests/files/bad-3-corrupt_lzma2.xz
 - Contient du shellscript appelé lors du build process (deb/rpm)
 - Modifie le code C avant la compilation pour appeler `_get_cpuid`
 - Et du shellcode injecté dans **liblzma** lors de la compilation
 - Exporte le symbole `_get_cpuid` mentionné plus tôt
 - Hijack la table d'appels de **RSA_public_decrypt**