

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**

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