Un algorithme de compression corrige une faille vieille de 20 ans

L'algorithme de Lempel-Ziv-Oberhumer (LZO) ne vous dit peut-être rien et pourtant il vient de battre un record en matière de sécurité informatique. En effet, ce système de compression de flux de données **créé en 1994** par Markus Oberhumer pour la NASA et notamment les modules martiens (dont Curiosity), comprenait dès son origine une vulnérabilité qui vient d'être corrigée. **Après 20 ans d'existence**.

Cet algorithme a subi plusieurs transformations au cours de ces années avec plusieurs déclinaisons, au point qu'il était très difficile à corriger. Il aura donc fallu attendre la version 2.07 de LZO pour patcher ce « vieux problème » qui autorisait **une saturation de la mémoire tampon** en jouant sur certaines variantes dites « sécurisées » du système de décompression avec des données malveillantes.

A la recherche de la faille perdue

Dans un blog, **Don Bailey**, CEO et co-fondateur de Lab Mouse Security, a donné un peu plus de détails sur ce vénérable bug. « *En réutilisant le code qui est connu pour bien fonctionner, surtout les algorithmes hautement optimisés, les projets peuvent être vulnérables car la confiance dans ce code n'est pas remise en cause* », affirme le consultant. Ce dernier a l'habitude de travailler sur la sécurité des technologies mobiles, l'Internet des objets et les systèmes embarqués. Il précise que « *les implémentations de LZO peuvent être sensiblement différents, mais chaque variante est vulnérable de la même façon* ». Il demande donc aux utilisateurs **d'évaluer leurs algorithmes pour savoir s'ils sont corrigés**. Pour cela, il donne différentes méthodes aux administrateurs pour savoir si leurs infrastructures est vulnérable à la faille et ensuite comment la corriger.

Il est à noter que LZO est une bibliothèque de compression qui a trouvé sa place dans bon nombre de projets IT. On peut citer notamment **Android, OpenVPN, MPlayer2, Libav, le kernel Linux, mais également Junos de Juniper,** etc.

crédit photo © Pavel Ignatov – shutterstock

A lire aussi :

Une faille de sécurité vieille de 5 ans corrigée dans le noyau Linux

Une faille vieille de six ans découverte dans Explorer