Les disques durs chiffrés de Western Digital critiqués pour leurs failles de sécurité | Le Net Expert Informatique

Les disques durs chiffrés de Western Digital critiqués pour leurs failles de sécurité

Dans un papier publié le mois dernier, trois chercheurs en cybersécurité se sont penchés sur le chiffrement offert par plusieurs disques durs externes de la marque Western Digital. Les modèles testés sont vulnérables à des attaques permettant de contourner le chiffrement proposé.

Le chiffrement proposé par les disques durs Western Digital des gammes Passport et My Book souffre de nombreux défauts selon trois chercheurs en cybersécurité. Dans un papier publié il y a un mois, les trois experts se sont penchés sur les conditions d'implémentation du chiffrement dans les différents produits de ces deux gammes de disques durs externes, qui proposent un outil de chiffrement des données stockées sur le disque dur afin d'en protéger l'accès.
Ainsi, la plupart des disques de la gamme proposent un chiffrement s'appuyant sur un mot de passe connu par l'utilisateur. Ce mot de passe est haché grâce à la fonction de hachage SHA256 afin de générer une seconde clef, baptisée DEK (Data Encryption Key), stockée sur le disque et permettant de chiffrer ou déchiffrer les données lors de leur utilisation par l'utilisateur.

Nombreuses erreurs

Mais cette implémentation, étudiée par les chercheurs, souffre de nombreuses vulnérabilités qui rendent possible pour un attaquant expérimenté d'accéder aux données chiffrées sur le disque dur. Ainsi, dans un des modèles analysés, le mot de passe enregistré par l'utilisateur était stocké en clair sur le firmware de l'appareil.
Les chercheurs relèvent également des erreurs dans la génération des chiffres aléatoires utilisés pour le chiffrement des données, qui se basent sur l'horloge interne de l'ordinateur, ou encore la possibilité d'extraire le hash présent sur certains modèles, ce qui ouvre la possibilité d'une attaque par bruteforce. Ces vulnérabilités nécessitent néanmoins que l'attaquant ait physiquement accès au disque dur en question pour pouvoir être exploitées.
Les chercheurs expliquent avoir informé Western Digital des différentes failles trouvées sur les disques durs de la gamme, mais n'avoir aucune information quant à un éventuel correctif prévu par le constructeur.

Source :
http://www.zdnet.fr/actualites/les-disques-durs-chiffres-de-western-digital-critiques-pour-leurs-failles-de-securite-39826890.htm