Forum: Dépannage

Topic: KeePass Password Safe v2.35.

Subject: KeePass Password Safe v2.35.

Publié par: Garuda-3366

Contribution le : 11/01/2017 19:17:55

Bonjour,

La nouvelle version **2.35** de **KeePass Password Safe** introduit un certain nombre d'innovations. Parmi celles-ci, il en est une qui me laisse hésitant sur le meilleur paramétrage à adopter pour sécuriser la base de données :

Mon interrogation porte principalement sur la rubrique **"Transformation de clé"** (Key transformation) et le choix d'**Argon2** (qui offrirait une meilleure sécurité que **AES-KDF**). Rappelons que cette rubrique est accessible via le menu *Fichier/Paramètres de la base de données/(onglet) Sécurité / Transformation de clé / Fonction de dérivation de clé.*
Seulement, en sélectionnant **Argon2** à la place de **AES-KDF**, d'autres éléments de réglages apparaissent ainsi :
- Itérations : 2 (par défaut).
- Mémoire : 1 MB (par défaut)
- Parallélisme : 2 (par défaut).

Il est indiqué que plus le nombre d'itérations est élevé, plus les attaques en vue de découvrir le mot de passe (dictionnaire, divination) seront ardues (avec l'inconvénient de rendre plus long le chargement et l'enregistrement de la base de données en question). Soit, mais ce que je trouve étrange, c'est que le nombre d'itérations par défaut du programme est seulement de **2** avec **Argon2** alors qu'il est réglé par défaut à **6000** avec **AES-KDF**. La différence est de taille !

Je serai donc intéressé par tout éclairage sur le meilleur paramétrage possible que les connaisseurs voudront bien exprimer ici car je n'ai pas trouvé d'éléments de réponse satisfaisants sur le site de l'éditeur.
Avec mes remerciements anticipés.