

Se connecter

Proposer un contenu

Identifiant

Identifiant

Mot de passe

Mot de passe

☐ Connexion automatique

Se connecter

Pas de compte ? S'inscrire...

Journal : 100 100 itérations : ce que le vol des coffres LastPass dit du choix d'un gestionnaire

Posté par Seijiro le 10 octobre 2026 à 14:40. Licence CC By-SA.
Étiquettes : slop, mot_de_passe, sécurité, keepassxc, vaultwarden, chiffrement, seo



Je relisais la notice de LastPass sur l'incident de 2022, et un chiffre m'a arrêté.

Dans [sa notice du 22 décembre 2022](#), l'entreprise explique qu'une sauvegarde de données de coffres clients a été copiée. Elle précise que ces coffres contiennent « both unencrypted data, such as website URLs » et des champs chiffrés en AES 256 : identifiants, mots de passe, notes sécurisées, données de formulaires. Elle ajoute que le mot de passe maître n'est jamais connu d'elle, qu'un minimum de douze caractères est imposé depuis 2018, et qu'elle applique « 100,100 iterations of the Password-Based Key Derivation Function (PBKDF2) ».

C'est ce dernier nombre qui mérite qu'on s'arrête. La [fiche de l'OWASP sur le stockage des mots de passe](#) recommande aujourd'hui Argon2id avec au moins 19 Mio de mémoire, deux itérations et un parallélisme de 1, et réserve PBKDF2 aux contextes qui exigent la conformité FIPS, avec au moins 600 000 itérations en HMAC-SHA-256. Entre 100 100 et 600 000, il y a un facteur six, et ce facteur se paie en temps de calcul chez l'attaquant qui détient déjà le fichier.

La leçon n'est pas que LastPass a mal fait son travail en 2022 : c'était un paramétrage courant à l'époque. Elle est que la robustesse d'un coffre volé ne se joue pas sur le fait qu'il soit chiffré, mais sur une poignée de paramètres de dérivation que l'utilisateur ne voit jamais et ne choisit pas.

D'où mon biais, qui n'est pas idéologique : avec [Kee-PassXC](#), la fonction de dérivation et ses paramètres sont dans l'interface, modifiables, et le format du fichier est documenté. Avec [Vaultwarden](#), on garde les clients Bitwarden sans confier le coffre à un tiers. Dans les deux cas, on peut lire et régler ce qui, ailleurs, est une décision prise pour vous et héritée de l'année de création du compte.

Deux réserves, pour ne pas vendre du rêve. S'auto-héberger ne supprime pas le risque, ça le déplace : sauvegardes, mises à jour et disponibilité deviennent votre problème, et un coffre perdu est aussi définitif qu'un coffre volé. Et la partie non chiffrée reste non chiffrée quel que soit le logiciel : savoir que vous aviez un compte quelque part n'est pas révoicable, contrairement à un mot de passe.

Ma question pour le fil : combien d'entre vous ont réellement regardé les paramètres de dérivation de leur gestionnaire plutôt que de garder les valeurs par défaut, et lesquels utilisez-vous ?

Pour celles et ceux que le versant hachage intéresse, avec les ordres de grandeur de vitesse selon le type d'empreinte, j'avais détaillé ça [sur mon site](#).

(5 commentaires) Markdown EPUB

J'ai pas regardé

Posté par pulkomandy (site web personnel, Mastodon) le 10 octobre 2026 à 15:49. Évalué à 5 (+3/-1).

Ma question pour le fil : combien d'entre vous ont réellement regardé les paramètres de dérivation de leur gestionnaire plutôt que de garder les valeurs par défaut, et lesquels utilisez-vous ?



J'ai pas regardé la config de mon KeePassXC.

Pour Vaultwarden il me semble avoir vu des alertes dans l'interface web indiquant que la configuration en place n'était plus conforme aux recommandations actuelles et qu'il fallait faire des modifications (mais c'est sur un truc où je n'ai pas la main pour faire ce genre de config).

Pour moi la conclusion est: si jamais votre coffre de mots de passe a été volé, même s'il est chiffré, tout ce que ça vous apporte, c'est du temps pour renouveler tous les mots de passe avant que le chiffrement du coffre puisse être cassé. Quelques mois ou années si le coffre est bien chiffré avec des bons paramètres, peut-être seulement quelques jours ou quelques heures dans le cas contraire. Mais dans tous les cas, un jour le coffre sera cassé.

Répondre

Mauvaise question

Posté par fork_bomb le 10 octobre 2026 à 16:06. Évalué à 5 (+4/-0).

Ma question pour le fil : combien d'entre vous ont réellement regardé les paramètres de dérivation de leur gestionnaire plutôt que de garder les valeurs par défaut, et lesquels utilisez-vous ?



Ton LLM pose la mauvaise question : la tendance en cryptographie est plutôt à rendre les outils non paramétrables, avec les choix d'algorithmes et de paramètres faits par des experts. La question devrait donc plutôt être pourquoi c'est paramétrable, et pourquoi les paramètres par défaut ne sont pas les plus sûrs.

Répondre

Ça m'intéresse, tu peux détailler svp ?

Posté par Luc-Skywalker le 10 octobre 2026 à 16:19. Évalué à 4 (+2/-0).

C'est ce dernier nombre qui mérite qu'on s'arrête. La fiche de l'OWASP sur le stockage des mots de passe recommande aujourd'hui Argon2id avec au moins 19 Mio de mémoire, deux itérations



et un parallélisme de 1, et réserve PBKDF2 aux contextes qui exigent la conformité FIPS, avec au moins 600 000 itérations en HMAC-SHA-256. Entre 100 100 et 600 000, il y a un facteur six, et ce facteur se paie en temps de calcul chez l'attaquant qui détient déjà le fichier.

c'est un peu obscur, j'ai besoin de tes lumières.
Merci

--
"Si tous les cons volaient, il ferait nuit" F. Dard

Répondre

Autopromotion

Posté par **Glandos** le 10 octobre 2026 à 18:12. Évalué à 3 (+1/-0).

Pour ceux qui veulent une sauvegarde auto-suffisante :



https://framagit.org/Glandos/rbw_portable

C'est probablement très mal documenté, n'hésitez à proposer mieux :)

Répondre

Changement params de chiffrement de la BD

Posté par **lolop (site web personnel)** le 10 octobre 2026 à 18:41. Évalué à 3 (+1/-0).

Utilisateur de KeePassXC, j'ai laissé les paramètres par défaut.



Mais dans KeePassXC, si tu trouves a posteriori que c'est insuffisant, tu peux aller changer les paramètres de chiffrement.

--
Votez les 30 juin et 7 juillet, en connaissance de cause.
<http://www.pointal.net/VotesDeputesRN>

Répondre

Envoyer un commentaire

Suivre le flux des commentaires

Note : les commentaires appartiennent à celles et ceux qui les ont postés. Nous n'en sommes pas responsables.

Revenir en haut de page

Derniers commentaires

- Re: Slovénie
- Re: Slovénie
- Re: Purée
- Re: Question naïve
- Changement param...
- Re: Architecture de l...
- Re: Architecture de l...
- Re: Question naïve
- Autopromotion
- Re: Quel clown :/
- Quel clown :/
- Re: dns

Étiquettes (tags) populaires

- intelligence_artificielle
- slop
- merdification
- grands_modèles_de...
- états-unis
- chine
- jihad_butlérien
- capitalisme
- bigtech
- politique
- administration_fran...
- meta

Sites amis

- Agenda du Libre
- April
- Éditions D-BookeR
- Éditions Diamond
- Éditions Eyrolles
- Éditions ENI
- En Vente Libre
- Framasoft
- La Quadrature du Net
- Lea-Linux
- Open Source Initiative
- Imprimerie Grafik Plus

À propos de LinuxFr.org

- Mentions légales
- Faire un don
- L'équipe de LinuxFr....
- Informations sur le s...
- Aide / Foire aux que...
- Suivi des suggestion...
- Wiki du site
- Règles de modération
- Statistiques
- API pour le développ...
- Code source du site
- Plan du site