SÉCURITÉ > ENCRYPTION

Algorithmes KDF

Algorithmes KDF

Bitwarden utilise d'abord les fonctions de dérivation de clé (KDF) lors de la création du compte pour dériver une clé principale pour le compte à partir du mot de passe principal entré, qui sert d'entrée pour un hachage du mot de passe principal pour le compte (en savoir plus). Chaque fois qu'un utilisateur est authentifié, par exemple lors du déverrouillage d'un coffre -fort ou de la satisfaction d'une nouvelle invite de mot de passe principal , le processus est répété afin que le hachage nouvellement dérivé puisse être comparé au hachage dérivé d'origine. Si elles correspondent, l'utilisateur est authentifié.

Les KDF sont utilisés dans cette capacité pour contrer les attaques par force brute ou par dictionnaire contre un mot de passe principal. Les KDF obligent les machines de l'attaquant à calculer un nombre non négligeable de hachages pour chaque essai de mot de passe, augmentant ainsi le coût pour l'attaquant.

Deux algorithmes KDF sont actuellement disponibles pour utilisation dans Bitwarden; **PBKDF2** et **Argon2**. Chaque algorithme dispose d'une sélection d'options disponibles qui peuvent être utilisées pour augmenter le temps et les dépenses, ou "facteur de travail", imposés à l'attaquant.

PBKDF2

La fonction de dérivation de clé basée sur le mot de passe 2 (PBKDF2) est recommandée par le NIST et, telle qu'implémentée par Bitwarden, satisfait aux exigences FIPS-140 tant que les valeurs par défaut ne sont pas modifiées.

PBKDF2, tel qu'implémenté par Bitwarden, fonctionne en salant votre mot de passe principal avec votre nom d'utilisateur et en exécutant la valeur résultante à travers un algorithme de hachage unidirectionnel (HMAC-SHA-256) pour créer un hachage de longueur fixe. Cette valeur est à nouveau salée avec votre nom d'utilisateur et hachée un nombre configurable de fois (**Itérations KDF**). La valeur résultante après toutes les itérations est votre clé principale, qui sert d'entrée pour le hachage du mot de passe principal utilisé pour authentifier cet utilisateur chaque fois qu'il se connecte (en savoir plus).

Par défaut, Bitwarden est configuré pour itérer 600 000 fois, comme recommandé par OWASP pour les implémentations HMAC-SHA-256. Tant que l'utilisateur ne définit pas cette valeur plus bas, la mise en œuvre est conforme à FIPS-140, mais voici quelques conseils si vous choisissez de modifier vos paramètres :

- Plus d'itérations KDF augmenteront **à la fois** le temps qu'il faudra à un attaquant pour craquer un mot de passe **et** le temps qu'il faudra à un utilisateur légitime pour se connecter.
- Nous vous recommandons d'augmenter la valeur par incréments de 100 000 et de tester tous vos appareils.

Argon2id

Argon2 est le gagnant de la Compétition de Hachage de Mot de Passe de 2015. Il existe trois versions de l'algorithme, et Bitwarden a mis en œuvre Argon2id comme recommandé par OWASP. Argon2id est un hybride d'autres versions, utilisant une combinaison d'accès à la mémoire dépendant des données et indépendant des données, ce qui lui confère une partie de la résistance d'Argon2i aux attaques de synchronisation de cache par canal latéral et une grande partie de la résistance d'Argon2d aux attaques de craquage par GPU (source).

Argon2, tel qu'implémenté par Bitwarden, fonctionne en salant votre mot de passe principal avec votre nom d'utilisateur et en exécutant la valeur résultante à travers un algorithme de hachage unidirectionnel (BLAKE2b) pour créer un hachage de longueur fixe.

Argon2 alloue ensuite une portion de mémoire (**mémoire KDF**) et la remplit avec le hachage calculé jusqu'à ce qu'elle soit pleine. Cela est répété, en commençant dans la portion de mémoire suivante où il s'est arrêté en premier, un nombre de fois de manière itérative (**Itérations KDF**) sur un nombre de fils (**Parallélisme KDF**). La valeur résultante après toutes les itérations, est votre clé principale, qui sert d'entrée pour le hachage du mot de passe principal utilisé pour authentifier cet utilisateur chaque fois qu'ils se connectent (en savoir plus).

Par défaut, Bitwarden est configuré pour allouer 64 MiB de mémoire, l'itérer 3 fois et le faire sur 4 fils d'exécution. Ces valeurs par défaut sont supérieures aux recommandations actuelles de l'OWASP, mais voici quelques conseils si vous choisissez de modifier vos paramètres :

- Augmenter les **itérations KDF** augmentera le temps d'exécution de manière linéaire.
- La quantité de **Parallélisme KDF** que vous pouvez utiliser dépend du CPU de votre machine. Généralement, Max. Parallélisme = Nombre de cœurs x 2.
- iOS limite la mémoire de l'application pour l'autocomplétion. Augmenter les itérations par défaut de 64 MB peut entraîner des erreurs lors du déverrouillage du coffre avec l'autoremplissage.

Changer l'algorithme KDF

> **ⓘ Note**
>
> **2023-02-14**: Argon2 est pris en charge par les clients Bitwarden version 2023.2.0 et ultérieure, et passer à Argon2 via le coffre web pourrait signifier que les autres clients ne pourront pas charger votre coffre jusqu'à ce qu'ils soient mis à jour, généralement dans la semaine suivant la sortie.

Pour changer votre algorithme KDF, naviguez vers **Paramètres → Sécurité → Clés** sur la page du coffre web. Changer l'algorithme va ré-encrypter la clé symétrique protégée et mettre à jour le hachage d'authentification, tout comme un changement normal de mot de passe principal, mais ne régénérera pas la clé de chiffrement symétrique donc les données du coffre ne seront pas ré-encryptées. Voir ici pour des informations sur le re-chiffrement de vos données.

Lorsque vous changez d'algorithme, vous serez déconnecté de tous les clients. Bien que le risque impliqué dans la régénération de votre clé de chiffrement n'existe pas lors du changement d'algorithme, nous recommandons toujours de exporter votre coffre au préalable.

Faibles itérations KDF

Dans la version 2023.2.0, Bitwarden a augmenté le nombre par défaut d'itérations KDF pour les comptes utilisant l'algorithme PBKDF2 à 600 000, conformément aux directives OWASP mises à jour. Cela renforce le chiffrement du coffre contre les pirates armés d'appareils de plus en plus puissants. Si vous utilisez l'algorithme PBKDF2 et que vous avez défini les itérations KDF en dessous de 600 000, vous recevrez un message d'avertissement vous encourageant à augmenter vos paramètres KDF.

> **⚠ Warning**
>
> Avant de faire des modifications aux paramètres de chiffrement, il est recommandé de sauvegarder d'abord vos données de coffre individuelles. Voir Exporter les Données du Coffre pour plus d'informations.

Pour maintenir le chiffrement à connaissance zéro, ni Bitwarden ni les administrateurs ne peuvent modifier les paramètres de sécurité de votre compte ou les paramètres de chiffrement de votre coffre. Si vous voyez ce message, sélectionnez le bouton **Mettre à jour les paramètres KDF**

et augmentez soit vos itérations PBKDF2 à au moins 600 000, soit changez votre algorithme KDF pour Argon2id avec les paramètres par défaut. Lorsque vous enregistrez ces modifications, vous serez déconnecté de tous les clients, alors assurez-vous que vous connaissez votre mot de passe principal et que votre méthode d'identifiant en deux étapes est accessible.

Modifier le nombre d'itérations peut aider à protéger votre mot de passe principal contre une force brute par un attaquant, cependant, cela ne doit pas être considéré comme un substitut à l'utilisation d'un mot de passe principal fort dès le départ. Un mot de passe principal fort est toujours la première et la meilleure ligne de défense pour votre compte Bitwarden.