bitwarden | Article du Centre d'Aide

SÉCURITÉ

Cryptage

Afficher dans le centre d'aide:
https://bitwarden.com/help/what-encryption-is-used/

Cryptage

Bitwarden utilise le chiffrement AES-CBC 256 bits pour les données de votre coffre, et PBKDF2 SHA-256 ou Argon2 pour dériver votre clé de chiffrement.

Bitwarden **toujours** crypte et/ou hache vos données sur votre appareil local avant que quoi que ce soit soit envoyé aux serveurs cloud pour stockage. **Les serveurs Bitwarden sont uniquement utilisés pour stocker des données cryptées.** Pour plus d'informations, voir Stockage.

Les données du coffre ne peuvent être déchiffrées qu'à l'aide de la clé dérivée de votre mot de passe principal. Bitwarden est une solution de chiffrement à connaissance zéro, ce qui signifie que vous êtes la seule partie ayant accès à votre clé et la capacité de déchiffrer les données de votre coffre.

> **Tip**
>
> Nous vous encourageons à visiter notre Page de Cryptographie Interactive pour voir par vous-même comment Bitwarden crypte vos données.
>
> Si vous souhaitez en savoir plus sur la manière dont ces clés de chiffrement sont utilisées pour protéger votre coffre, vous pouvez également consulter notre Livre Blanc sur la Sécurité.

AES-CBC

AES -CBC (cipher block chaining) , utilisé pour chiffrer les données du coffre-fort, est une norme de cryptographie utilisée par le gouvernement américain et d'autres agences gouvernementales du monde entier pour protéger les données top secrètes. Avec une mise en œuvre appropriée et une clé de chiffrement forte (votre mot de passe principal), AES est considéré comme inviolable.

PBKDF2

PBKDF2 SHA-256 est utilisé pour dériver la clé de chiffrement à partir de votre mot de passe principal, cependant vous pouvez choisir Argon2 comme alternative. Bitwarden sale et hache votre mot de passe principal avec votre adresse de courriel **localement**, avant la transmission à nos serveurs. Une fois qu'un serveur Bitwarden reçoit le mot de passe haché, il est salé à nouveau avec une valeur aléatoire cryptographiquement sécurisée, haché à nouveau, et stocké dans notre base de données.

Le nombre d'itérations par défaut utilisé avec PBKDF2 est de 600 001 itérations sur le client (le nombre d'itérations côté client est configurable à partir des paramètres de votre compte), puis 100 000 itérations supplémentaires lorsqu'il est stocké sur nos serveurs (pour un total de 700 001 itérations par défaut). La clé de l'organisation est partagée via RSA-2048.

> **Tip**
>
> Le nombre d'itérations par défaut utilisé par Bitwarden a été augmenté en février 2023. Les comptes créés après cette heure utiliseront 600 001, cependant si vous avez créé votre compte avant cela, vous devriez augmenter le nombre d'itérations. Les instructions pour ce faire peuvent être trouvées dans la section suivante.

Les fonctions de hachage utilisées sont des hachages unidirectionnels, ce qui signifie qu'elles **ne peuvent pas être rétro-conçues** par quiconque chez Bitwarden pour révéler votre mot de passe principal. Même si Bitwarden était piraté, il n'y aurait aucune méthode par laquelle votre mot de passe principal pourrait être obtenu.

Changer les itérations KDF

Bitwarden utilise un paramètre par défaut sécurisé, comme mentionné ci-dessus, cependant vous pouvez changer le nombre d'itérations depuis le menu **Paramètres** → **Sécurité** → **Clés** du coffre web.

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. La modification du

nombre d'itérations 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.

Régler vos itérations KDF trop haut pourrait entraîner une mauvaise performance lors de la connexion (et du déverrouillage) de Bitwarden sur des appareils avec des CPU plus lents. Nous vous recommandons d'augmenter la valeur par incréments de 100 000, puis de tester tous vos appareils.

Lorsque vous changez le nombre d'itérations, 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 du nombre d'Itérations KDF, nous recommandons toujours de exporter votre coffre au préalable.

Argon2id

Argon2, le gagnant de la Compétition de Hachage de Mot de Passe de 2015, est disponible en tant qu'alternative à PBKDF2 (en savoir plus). 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).

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.

> **Note**
> Les utilisateurs d'Argon2id avec une valeur de mémoire KDF supérieure à 48 Mo recevront un dialogue d'avertissement chaque fois que le remplissage automatique iOS est initié ou qu'un nouveau Send est créé via la feuille de partage. Pour éviter ce message, ajustez les paramètres Argon2id ou activez déverrouiller avec la biométrie.

Bibliothèques crypto invoquées

Bitwarden n'écrit aucun code cryptographique. Bitwarden n'invoque que le crypto provenant de bibliothèques crypto populaires et réputées qui sont écrites et maintenues par des experts en cryptographie. Les bibliothèques crypto suivantes sont utilisées :

- JavaScript (Coffre Web, extension de navigateur, bureau, et CLI)
  - Crypto Web
  - Node.js crypto
  - Fonderie
- C# (Mobile)
  - CommonCrypto (iOS, Apple)
  - Javax.Crypto (Android, Oracle)
  - BouncyCastle (Android)