SICHERHEIT

KDF-Algorithmen

KDF-Algorithmen

Bitwarden verwendet zuerst Key Derivation Functions (KDFs) bei der Kontoerstellung, um einen Master-Schlüssel für das Konto aus dem eingegebenen Master-Passwort abzuleiten, das als Eingabe für einen Master-Passwort-Hash für das Konto dient (mehr erfahren). Immer wenn ein Benutzer authentifiziert wird, zum Beispiel beim Entsperren eines Tresors oder beim Erfüllen der Master-Passwort erneute Aufforderung, wird der Prozess wiederholt, damit der neu abgeleitete Hash mit dem ursprünglich abgeleiteten Hash verglichen werden kann. Wenn sie übereinstimmen, wird der Benutzer authentifiziert.

KDFs werden in dieser Kapazität verwendet, um Brute-Force- oder Wörterbuchangriffe gegen ein Master-Passwort zu erschweren. KDFs zwingen die Maschinen eines Angreifers dazu, eine nicht unerhebliche Nummer von Hashes für jede Passwort-Vermutung zu berechnen, was die Kosten für den Angreifer erhöht.

Zwei KDF-Algorithmen sind derzeit für die Verwendung in Bitwarden verfügbar; **PBKDF2** und **Argon2**. Jeder Algorithmus hat eine Auswahl an verfügbaren Optionen, die verwendet werden können, um die Zeit und die Kosten, oder den "Arbeitsfaktor", zu erhöhen, der dem Angreifer auferlegt wird.

PBKDF2

Die passwortbasierte Schlüsselableitungsfunktion 2 (PBKDF2) wird vom NIST empfohlen und erfüllt, wie von Bitwarden implementiert, die FIPS-140-Anforderungen, solange die Standardwerte nicht geändert werden.

PBKDF2, wie es von Bitwarden implementiert wird, funktioniert, indem Ihr Master-Passwort mit Ihrem Benutzernamen gesalzen und der resultierende Wert durch einen Einweg-Hash-Algorithmus (HMAC-SHA-256) geleitet wird, um einen Hash mit fester Länge zu erstellen. Dieser Wert wird erneut mit Ihrem Benutzernamen gesalzen und eine konfigurierbare Anzahl von Malen gehasht (**KDF-Iterationen**). Der resultierende Wert nach allen Iterationen ist Ihr Master-Schlüssel, der als Eingabe für den Master-Passwort-Hash dient, der verwendet wird, um diesen Benutzer bei jeder Anmeldung zu authentifizieren (mehr erfahren).

Standardmäßig ist Bitwarden so eingestellt, dass es 600.000 Mal iteriert, wie von OWASP für HMAC-SHA-256-Implementierungen empfohlen. Solange der Benutzer diesen Wert nicht niedriger setzt, ist die Implementierung FIPS-140-konform, aber hier sind einige Tipps, falls Sie sich entscheiden, Ihre Einstellungen zu ändern:

- Weitere KDF-Iterationen erhöhen **sowohl** die Zeit, die ein Angreifer zum Knacken eines Passworts benötigt **, als auch** die Zeit, die ein legitimer Benutzer zum Anmelden benötigt.
- Wir empfehlen, dass Sie den Wert in Schritten von 100.000 erhöhen und alle Ihre Geräte testen.

Argon2id

Argon2 ist der Gewinner des 2015 Passwort Hashing Wettbewerbs. Es gibt drei Versionen des Algorithmus und Bitwarden hat Argon2id implementiert wie von OWASP empfohlen. Argon2id ist eine Hybridversion anderer Versionen und verwendet eine Kombination aus datenabhängigen und datenunabhängigen Speicherzugriffen, was ihm einen Teil der Widerstandsfähigkeit von Argon2i gegen Seitenkanal-Cache-Timing-Angriffe und einen Großteil der Widerstandsfähigkeit von Argon2d gegen GPU-Cracking-Angriffe verleiht (Quelle).

Argon2, wie von Bitwarden implementiert, funktioniert, indem Ihr Master-Passwort mit Ihrem Benutzernamen gesalzen und der resultierende Wert durch einen Einweg-Hash-Algorithmus (BLAKE2b) geleitet wird, um einen Hash mit fester Länge zu erstellen.

Argon2 weist dann einen Teil des Speichers (**KDF-Speicher**) zu und füllt ihn mit dem berechneten Hash, bis er voll ist. Dies wird wiederholt, beginnend im nachfolgenden Teil des Speichers, wo es im ersten aufgehört hat, eine Anzahl von Malen iterativ (**KDF-Iterationen**) über eine Anzahl von Threads (**KDF-Parallelität**). Der resultierende Wert nach allen Iterationen ist Ihr Master-Schlüssel, der als Eingabe für den Master-Passwort-Hash dient, der verwendet wird, um diesen Benutzer bei jeder Anmeldung zu authentifizieren (mehr erfahren).

Standardmäßig ist Bitwarden so eingestellt, dass es 64 MiB Speicher zuweist, 3 Mal darüber iteriert und dies über 4 Threads tut. Diese Standardwerte liegen über den aktuellen OWASP-Empfehlungen, aber hier sind einige Tipps, sollten Sie sich entscheiden, Ihre Einstellungen zu ändern:

- Eine Erhöhung der **KDF-Iterationen** wird die Laufzeit linear erhöhen.
- Die Menge an **KDF-Parallelität**, die Sie verwenden können, hängt von der CPU Ihres Computers ab. Im Allgemeinen, Max. Parallelismus = Anzahl der Kerne x 2.
- iOS begrenzt den Arbeitsspeicher für die Autofill-Funktion. Eine Erhöhung der Iterationen von den standardmäßigen 64 MB kann zu Fehlern führen, während der Tresor mit Autofill entsperrt wird.

Ändern des KDF-Algorithmus

> **Note**
>
> **2023-02-14**: Argon2 wird von Bitwarden Clients Version 2023.2.0 und später unterstützt, und der Wechsel zu Argon2 über den Web-Tresor könnte bedeuten, dass andere Clients Ihren Tresor nicht laden können, bis sie aktualisiert sind, normalerweise innerhalb einer Woche nach der Veröffentlichung.

Um Ihren KDF-Algorithmus zu ändern, navigieren Sie zu der **Einstellungen** → **Sicherheit** → **Schlüssel** Seite des Web-Tresors. Die Änderung des Algorithmus wird den geschützten symmetrischen Schlüssel neu verschlüsseln und den Authentifizierungshash aktualisieren, ähnlich wie eine normale Änderung des Master-Passworts, aber der symmetrische Verschlüsselungsschlüssel wird nicht erneuert, sodass die Daten im Tresor nicht neu verschlüsselt werden. Siehe hier für Informationen zur erneuten Verschlüsselung Ihrer Daten.

Wenn Sie den Algorithmus ändern, werden Sie von allen Clients abgemeldet. Obwohl das Risiko, das bei der Erneuerung Ihres Verschlüsselungsschlüssels besteht, beim Wechsel des Algorithmus nicht besteht, empfehlen wir dennoch, vorher Ihren Tresor zu exportieren.

Niedrige KDF-Iterationen

In der 2023.2.0 Version hat Bitwarden die Standardanzahl der KDF-Iterationen für Konten, die den PBKDF2 Algorithmus verwenden, gemäß den aktualisierten OWASP-Richtlinien auf 600.000 erhöht. Dies stärkt die Tresor-Verschlüsselung gegen Hacker, die mit zunehmend leistungsfähigen Geräten bewaffnet sind. Wenn Sie den PBKDF2-Algorithmus verwenden und die KDF-Iterationen unter 600.000 eingestellt haben, erhalten Sie eine Warnmeldung, die Sie auffordert, Ihre KDF-Einstellungen zu erhöhen.

> **Warning**
>
> Bevor Sie Änderungen an den Verschlüsselungseinstellungen vornehmen, wird empfohlen, dass Sie zuerst Ihre individuellen Tresor-Daten sichern. Siehe Export Tresor Daten für weitere Informationen.

Um die Verschlüsselung mit Null-Wissen aufrechtzuerhalten, können weder Bitwarden noch Administratoren Ihre Kontosicherheits- oder Tresorverschlüsselungseinstellungen ändern. Wenn Sie diese Nachricht sehen, wählen Sie die Schaltfläche **KDF-Einstellungen aktualisieren** und erhöhen Sie entweder Ihre PBKDF2-Iterationen auf mindestens 600.000, oder ändern Sie Ihren KDF-Algorithmus zu Argon2id mit Standard-Einstellungen. Wenn Sie diese Änderungen speichern, werden Sie von allen Clients abgemeldet, stellen Sie also sicher, dass Sie Ihr Master-Passwort kennen und dass Ihre zweistufige Zugangsdaten Methode zugänglich ist.

Das Ändern der Iterationsanzahl kann dabei helfen, Ihr Master-Passwort vor einem Brute-Force-Angriff durch einen Angreifer zu schützen, sollte jedoch nicht als Ersatz für die Verwendung eines starken Master-Passworts von Anfang an betrachtet werden. Ein starkes Master-Passwort ist immer die erste und beste Verteidigungslinie für Ihr Bitwarden-Konto.