bitwarden | Artikel Helpcentrum

BEVEILIGING

KDF-algoritmen

Weergeven in het Helpcentrum:
https://bitwarden.com/help/kdf-algorithms/

KDF-algoritmen

Bitwarden gebruikt eerst Key Derivation Functions (KDF's) bij het aanmaken van een account om een hoofdsleutel voor het account af te leiden uit het ingevoerde hoofdwachtwoord, dat als invoer dient voor een hoofdwachtwoord hash voor het account(meer informatie). Telkens wanneer een gebruiker wordt geauthenticeerd, bijvoorbeeld bij het ontgrendelen van een kluis of het bevredigen van een hoofdwachtwoord re-prompt, wordt het proces herhaald zodat de nieuw afgeleide hash kan worden vergeleken met de oorspronkelijk afgeleide hash. Als ze overeenkomen, is de gebruiker geverifieerd.

KDF's worden in deze hoedanigheid gebruikt om brute-force of woordenboekaanvallen tegen een hoofdwachtwoord te dwarsbomen. KDF's dwingen de machines van een aanvaller om een niet-triviaal aantal hashes te berekenen voor elk geraden wachtwoord, met toenemende kosten voor de aanvaller.

Er zijn momenteel twee KDF-algoritmen beschikbaar voor gebruik in Bitwarden: **PBKDF2** en **Argon2**. Elk algoritme heeft een aantal opties die gebruikt kunnen worden om de tijd en kosten, of "werkfactor", voor de aanvaller te verhogen.

PBKDF2

Password-Based Key Derivation Function 2 (PBKDF2) wordt aanbevolen door NIST en voldoet, zoals geïmplementeerd door Bitwarden, aan de FIPS-140-vereisten zolang de standaardwaarden niet worden gewijzigd.

PBKDF2, zoals geïmplementeerd door Bitwarden, werkt door je hoofdwachtwoord te salten met je gebruikersnaam en de resulterende waarde door een eenrichtings hash-algoritme (HMAC-SHA-256) te laten lopen om een hash met een vaste lengte te maken. Deze waarde wordt opnieuw gezouten met je gebruikersnaam en een instelbaar aantal keren gehasht**(KDF iteraties**). De resulterende waarde na alle iteraties is uw hoofdsleutel, die dient als invoer voor de hoofdwachtwoord hash die wordt gebruikt om die gebruiker te verifiëren wanneer hij inlogt(meer informatie).

Standaard is Bitwarden ingesteld om 600.000 keer te itereren, zoals aanbevolen door OWASP voor HMAC-SHA-256-implementaties. Zolang de gebruiker deze waarde niet lager instelt, voldoet de implementatie aan FIPS-140, maar hier zijn enkele tips voor het geval je ervoor kiest om je instellingen te wijzigen:

- Meer KDF iteraties verhogen **zowel** de tijd die een aanvaller nodig heeft om een wachtwoord te kraken **als** de tijd die een legitieme gebruiker nodig heeft om in te loggen.
- We raden aan de waarde te verhogen in stappen van 100.000 en al je apparaten te testen.

Argon2id

Argon2 is de winnaar van de 2015 Password Hashing Competition. Er zijn drie versies van het algoritme en Bitwarden heeft Argon2id geïmplementeerd zoals aanbevolen door OWASP. Argon2id is een hybride van andere versies en gebruikt een combinatie van data-afhankelijke en data-onafhankelijke geheugentoegang. Hierdoor heeft het iets van de weerstand van Argon2i tegen side-channel cache timing aanvallen en veel van de weerstand van Argon2d tegen GPU cracking aanvallen(bron).

Argon2, zoals geïmplementeerd door Bitwarden, verzilt het hoofdwachtwoord met de gebruikersnaam en haalt de resulterende waarde door een eenrichtings hash-algoritme (BLAKE2b) om een hash met een vaste lengte te maken.

Argon2 wijst dan een deel van het geheugen toe**(KDF geheugen**) en vult dit met de berekende hash totdat het vol is. Dit wordt herhaald, beginnend in het volgende deel van het geheugen waar het in het eerste was gebleven, een aantal keren iteratief**(KDF iteraties**) over een aantal threads**(KDF parallellisme**). De resulterende waarde na alle iteraties is uw hoofdsleutel, die fungeert als invoer voor de hoofdwachtwoord hash die wordt gebruikt om die gebruiker te verifiëren wanneer hij inlogt(meer informatie).

Standaard is Bitwarden ingesteld om 64 MB geheugen toe te wijzen, er 3 keer overheen te gaan en dit over 4 threads te doen. Deze standaardinstellingen liggen boven de huidige aanbevelingen van OWASP, maar hier volgen enkele tips voor het geval je ervoor kiest om je instellingen te wijzigen:

- Als **de KDF iteraties** toenemen, neemt de looptijd lineair toe.

- De hoeveelheid **KDF parallellisme** die je kunt gebruiken hangt af van de CPU van je machine. Over het algemeen is Max. Parallellisme = aantal cores x 2.

- iOS beperkt het app-geheugen voor autofill. Het verhogen van iteraties van de standaard 64 MB kan leiden tot fouten tijdens het ontgrendelen van de kluis met autofill.

KDF-algoritme wijzigen

> **Note**
>
> **2023-02-14**: Argon2 wordt ondersteund door Bitwarden clients versie 2023.2.0 en later, en overstappen naar Argon2 via de web vault kan betekenen dat andere clients uw vault niet kunnen laden totdat ze zijn bijgewerkt, meestal binnen een week na de release.

Om je KDF-algoritme te wijzigen, navigeer je naar de **Instellingen** → **Beveiliging** → **Sleutels** pagina van de webkluis. Het veranderen van het algoritme zal de beschermde symmetrische sleutel opnieuw versleutelen en de authenticatie hash updaten, net zoals een normale hoofdwachtwoord verandering, maar zal de symmetrische encryptiesleutel niet roteren zodat kluisgegevens niet opnieuw versleuteld worden. Kijk hier voor informatie over het opnieuw versleutelen van je gegevens.

Als je van algoritme verandert, word je uitgelogd bij alle clients. Hoewel het risico van het roteren van je encryptiesleutel niet bestaat bij het veranderen van algoritme, raden we toch aan om je kluis vooraf te exporteren.

Lage KDF iteraties

In de release 2023.2.0 heeft Bitwarden het standaard aantal KDF-iteraties voor accounts die gebruikmaken van het PBKDF2-algoritme verhoogd naar 600.000, in overeenstemming met de bijgewerkte OWASP-richtlijnen. Dit versterkt de encryptie van kluizen tegen hackers die gewapend zijn met steeds krachtigere apparaten. Als je het PBKDF2 algoritme gebruikt en KDF iteraties lager dan 600.000 hebt ingesteld, krijg je een waarschuwing die je aanmoedigt om je KDF instellingen te verhogen.

> **⚠ Warning**
>
> Voordat u wijzigingen aanbrengt in de versleutelingsinstellingen, is het aan te raden om eerst een back-up te maken van uw individuele kluisgegevens. Zie Kluisgegevens exporteren voor meer informatie.

Om zero-knowledge-encryptie te handhaven, kunnen noch Bitwarden noch beheerders uw accountbeveiliging of kluisversleutelingsinstellingen wijzigen. Als dit bericht verschijnt, selecteer dan de knop **KDF-instellingen bijwerken** en verhoog de PBKDF2 iteraties tot minstens 600.000 of verander het KDF-algoritme in Argon2id met de standaardinstellingen. Als je deze wijzigingen opslaat, word je uitgelogd bij alle clients, dus zorg ervoor dat je je hoofdwachtwoord weet en dat je tweestaps inlogmethode toegankelijk is.

Het veranderen van het aantal iteraties kan helpen om je hoofdwachtwoord te beschermen tegen brute forcering door een aanvaller, maar moet niet worden gezien als een vervanging voor het gebruik van een sterk hoofdwachtwoord. Een sterk hoofdwachtwoord is altijd de eerste en beste verdedigingslinie voor uw Bitwarden-account.