bitwarden | Artículo del Centro de Ayuda

SEGURIDAD

Algoritmos KDF

Ver en el centro de ayuda:
https://bitwarden.com/help/kdf-algorithms/

Algoritmos KDF

Bitwarden primero utiliza Funciones de Derivación de Clave (KDFs) en la creación de la cuenta para derivar una clave maestra para la cuenta a partir de la contraseña maestra de entrada, que actúa como entrada para un hash de contraseña maestra para la cuenta (aprende más). Siempre que un usuario es autenticado, por ejemplo al desbloquear una caja fuerte o satisfacer la solicitud de repetición de la contraseña maestra, el proceso se repite para que el hash recién derivado pueda compararse con el hash originalmente derivado. Si coinciden, el usuario está autenticado.

Los KDF se utilizan en esta capacidad para frustrar ataques de fuerza bruta o de diccionario contra una contraseña maestra. Los KDF obligan a las máquinas del atacante a calcular un número no trivial de hashes para cada suposición de contraseña, aumentando el costo para el atacante.

Actualmente, dos algoritmos KDF están disponibles para su uso en Bitwarden; **PBKDF2** y **Argon2**. Cada algoritmo tiene una selección de opciones disponibles que se pueden utilizar para aumentar el tiempo y el costo, o "factor de trabajo", impuesto al atacante.

PBKDF2

La Función de Derivación de Clave Basada en Contraseña 2 (PBKDF2) es recomendada por NIST y, tal como está implementada por Bitwarden, cumple con los requisitos de FIPS-140 siempre y cuando no se cambien los valores predeterminados.

PBKDF2, tal como lo implementa Bitwarden, funciona salando tu contraseña maestra con tu nombre de usuario y ejecutando el valor resultante a través de un algoritmo de hash unidireccional (HMAC-SHA-256) para crear un hash de longitud fija. Este valor se vuelve a salar con tu nombre de usuario y se cifra un número configurable de veces (**Iteraciones KDF**). El valor resultante después de todas las iteraciones es tu clave maestra, que actúa como entrada para el hash de la contraseña maestra utilizado para autenticar a ese usuario cada vez que inician sesión (aprende más).

Por defecto, Bitwarden está configurado para iterar 600,000 veces, como recomendado por OWASP para las implementaciones de HMAC-SHA-256. Siempre y cuando el usuario no establezca este valor más bajo, la implementación cumple con FIPS-140, pero aquí hay algunos consejos en caso de que decida cambiar sus ajustes:

- Más iteraciones KDF aumentarán **tanto** el tiempo que le llevará a un atacante descifrar una contraseña **como** el tiempo que le llevará a un usuario legítimo iniciar sesión.

- Recomendamos que aumente el valor en incrementos de 100,000 y pruebe todos sus dispositivos.

Argon2id

Argon2 es el ganador de la Competencia de Hashing de Contraseña de 2015. Hay tres versiones del algoritmo, y Bitwarden ha implementado Argon2id como recomendado por OWASP. Argon2id es una combinación de otras versiones, utilizando una combinación de accesos a la memoria dependientes e independientes de los datos, lo que le da parte de la resistencia de Argon2i a los ataques de temporización de caché de canal lateral y gran parte de la resistencia de Argon2d a los ataques de cracking de GPU (fuente).

Argon2, tal como lo implementa Bitwarden, funciona salando tu contraseña maestra con tu nombre de usuario y ejecutando el valor resultante a través de un algoritmo de hash unidireccional (BLAKE2b) para crear un hash de longitud fija.

Argon2 luego asigna una porción de memoria (**memoria KDF**) y la llena con el hash calculado hasta que está llena. Esto se repite, comenzando en la siguiente porción de memoria donde se detuvo en la primera, un número de veces de manera iterativa (**Iteraciones KDF**) a través de un número de hilos (**Paralelismo KDF**). El valor resultante después de todas las iteraciones, es tu clave maestra, que actúa como entrada para el hash de la contraseña maestra utilizado para autenticar a ese usuario cada vez que inician sesión (aprende más).

Por defecto, Bitwarden está configurado para asignar 64 MiB de memoria, iterar sobre ella 3 veces y hacerlo en 4 hilos. Estos valores predeterminados están por encima de las recomendaciones actuales de OWASP, pero aquí hay algunos consejos en caso de que decidas cambiar tus ajustes:

- Aumentar las **Iteraciones KDF** aumentará el tiempo de ejecución de manera lineal.
- La cantidad de **Paralelismo KDF** que puedes usar depende de la CPU de tu máquina. Generalmente, Max. Paralelismo = Número de núcleos x 2.
- iOS limita la memoria de la aplicación para el autocompletado. Aumentar las iteraciones desde los 64 MB predeterminados puede resultar en errores al desbloquear la caja fuerte con autofill.

Cambiando el algoritmo KDF

> **Note**
>
> **2023-02-14**: Argon2 es compatible con la versión 2023.2.0 y posteriores de los clientes de Bitwarden, y cambiar a Argon2 a través de la caja fuerte web podría significar que otros clientes no podrán cargar tu caja fuerte hasta que se actualicen, normalmente dentro de una semana después del lanzamiento.

Para cambiar tu algoritmo KDF, navega a los **Ajustes** → **Seguridad** → **Claves** de la página de la caja fuerte web. Cambiar el algoritmo volverá a cifrar la clave simétrica protegida y actualizará el hash de autenticación, muy similar a un cambio normal de contraseña maestra, pero no rotará la clave de cifrado simétrico, por lo que los datos de la caja fuerte no serán cifrados de nuevo. Vea aquí para obtener información sobre cómo volver a cifrar sus datos.

Cuando cambies el algoritmo, se cerrará sesión en todos los clientes. Aunque el riesgo involucrado en rotar tu clave de cifrado no existe cuando cambias de algoritmo, aún recomendamos exportar tu caja fuerte de antemano.

Bajas iteraciones KDF

En la versión 2023.2.0, Bitwarden aumentó el número predeterminado de iteraciones KDF para las cuentas que utilizan el algoritmo PBKDF2 a 600,000, de acuerdo con las pautas actualizadas de OWASP. Esto fortalece la encriptación de la caja fuerte contra los hackers armados con dispositivos cada vez más potentes. Si está utilizando el algoritmo PBKDF2 y tiene las iteraciones KDF establecidas por debajo de 600,000, recibirá un mensaje de advertencia que le anima a aumentar sus ajustes KDF.

> **Warning**
>
> Antes de hacer cualquier cambio en los ajustes de cifrado, se recomienda que primero haga una copia de seguridad de los datos de su caja fuerte individual. Vea Exportar Datos de la Caja Fuerte para más información.

Para mantener la encriptación de cero conocimiento, ni Bitwarden ni los administradores pueden modificar los ajustes de seguridad de tu cuenta o los ajustes de encriptación de tu caja fuerte. Si ves este mensaje, selecciona el botón **Actualizar ajustes de KDF** y aumenta tus iteraciones de PBKDF2 al menos a 600,000, o cambia tu algoritmo de KDF a Argon2id con ajustes predeterminados. Cuando guardes estos cambios, se cerrará sesión en todos los clientes, así que asegúrate de que conoces tu contraseña maestra y que tu método de inicio de sesión de dos pasos es accesible.

Cambiar el recuento de iteraciones puede ayudar a proteger su contraseña maestra de ser forzada bruscamente por un atacante, sin embargo, no debe ser visto como un sustituto para usar una contraseña maestra fuerte en primer lugar. Una contraseña maestra fuerte es siempre la primera y mejor línea de defensa para tu cuenta de Bitwarden.