秘密解読

秘密解読

シークレットマネージャーは、マスターパスワードに加えて、アクセストークンを使用して、シークレットを復号化、編集、作成することができます。具体的には、これはここの例のようなシークレット注入シナリオで行われます。

概念的には、アクセストークンは2つのコンポーネント部分で構成されています：

- Bitwarden サーバーでの認証のためのクライアント ID とシークレットを含む**API キー**。
- あなたの組甕の対称暗号化キーを含む暗号化されたペイロードを復号化するために使用される、**ユニークな暗号化キー**。

アクセストークンが使用される場合、たとえば`bws get secret`のようなCLIコマンドを認証する場合など：

1. APIキーのクライアントIDとクライアントシークレットを含むリクエストがBitwardenサーバーに送信されます。
2. Bitwardenサーバーはこれらの資格情報を使用してクライアントセッションを認証し、暗号化されたペイロードを含むレスポンスをSendします。この暗号化されたペイロードには、組電の対称キーが含まれています。
3. 一度受け取ると、組織の対称キーは、アクセストークンのユニークな暗号化キーを使用してローカルで復号化されます。
4. `bws`コマンドで呼び出されるデータ、例えば秘密など、Bitwarden APIに対して後続のリクエストが送信されます。
5. Bitwardenは、リクエスト内のサービスアカウント識別子に基づいて、要求されたデータを提供できるかどうかを決定します。はい、場合によっては、暗号化されたデータを含むレスポンスがクライアントに送信されます。
6. データは、組織の対称キーを使用してローカルで復号化されます。関連する値は、例えば復号化された`"キー": ""`の値を環境変数に保存するなど、シークレットマネージャーの使用方法に関係なく使用されます。