ADMINISTRADOR DE SECRETOS > TUS SECRETOS

Descifrado de Secretos

Descifrado de Secretos

El Administrador de secretos puede usar tokens de acceso, además de la contraseña maestra, para descifrar, editar y crear secretos. Específicamente, esto se hace en escenarios de inyección de secretos como los ejemplos aquí.

Conceptualmente, los tokens de acceso constan de dos componentes:

- **Una clave API** que contiene una identificación de cliente y un secreto para la autenticación con los servidores Bitwarden.
- Una **clave de cifrado única**, que se utilizará para descifrar una carga útil cifrada que contiene la clave de cifrado simétrico de su organización.

Cuando se utiliza un token de acceso, por ejemplo al autenticar un comando de ILC como `bws obtener secreto`:

1. Se envía una solicitud a los servidores de Bitwarden que contiene el id del cliente y el secreto del cliente de la clave API.
2. Los servidores de Bitwarden utilizan estas credenciales para autenticar la sesión del cliente, y enviar una respuesta que contiene una carga útil cifrada. Esta carga cifrada contiene la clave simétrica de la organización.
3. Una vez recibida, la clave simétrica de la organización se descifra localmente utilizando la clave de cifrado única del token de acceso.
4. Se envía una solicitud posterior a las API de Bitwarden para los datos solicitados en el comando `bws`, por ejemplo, un secreto.
5. Bitwarden determina si los datos solicitados pueden proporcionarse en base a un identificador de cuenta de servicio en la solicitud. Si es así, se envía una respuesta al cliente con los datos encriptados.
6. Los datos se descifran localmente utilizando la clave simétrica de la organización. Los valores relevantes se utilizan independientemente de cómo utilice Secrets Manager, por ejemplo, guardando un valor `"clave": ""` descifrado en una variable de entorno.