GEHEIMEN MANAGER > JOUW GEHEIMEN

Geheime ontcijfering

Geheime ontcijfering

Secrets Manager kan naast hoofdwachtwoorden ook toegangsmunten gebruiken om geheimen te ontcijferen, bewerken en aanmaken. Specifiek wordt dit gedaan in secrets injection scenario's zoals de voorbeelden hier.

Conceptueel bestaan toegangstokens uit twee componenten:

- **Een API-sleutel** die een client-id en geheim bevat voor verificatie met Bitwarden-servers.
- **Een unieke coderingssleutel**, die wordt gebruikt om een versleutelde payload met de symmetrische coderingssleutel van je organisatie te ontsleutelen.

Wanneer een toegangstoken wordt gebruikt, bijvoorbeeld bij het authenticeren van een CLI commando zoals `bws get secret`:

1. Er wordt een verzoek naar de Bitwarden-servers gestuurd met de client-id en het client-secret van de API-sleutel.
2. Bitwarden-servers gebruiken deze gegevens om de clientsessie te verifiëren en sturen een antwoord met een versleutelde payload. Deze versleutelde payload bevat de symmetrische sleutel van de organisatie.
3. Na ontvangst wordt de symmetrische sleutel van de organisatie lokaal gedecodeerd met de unieke coderingssleutel van het toegangstoken.
4. Vervolgens wordt een verzoek gestuurd naar de Bitwarden API's voor de gegevens die worden gevraagd in het `bws-commando`, bijvoorbeeld een geheim.
5. Bitwarden bepaalt of de opgevraagde gegevens kunnen worden geleverd op basis van een service account identifier in het verzoek. Zo ja, dan wordt er een antwoord naar de cliënt gestuurd met de versleutelde gegevens.
6. De gegevens worden lokaal gedecodeerd met de symmetrische sleutel van de organisatie. Relevante waarden worden gebruikt hoe je Secrets Manager ook gebruikt, bijvoorbeeld het opslaan van een gedecodeerde `"sleutel": ""` waarde naar een omgevingsvariabele.