RFC 8959 : The "secret-token" URI Scheme

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 30 janvier 2021

Date de publication du RFC : Janvier 2021

https://www.bortzmeyer.org/8959.html

Enregistrer une clé privée (ou tout autre secret) dans un dépôt public (par exemple sur GitHub) est un gag courant. La nature des VCS fait qu'il est souvent difficile de retirer cette clé. Pour limiter un peu les dégâts, ce RFC enregistre un nouveau plan d'URI, `secret-token:`, qui permettra de marquer ces secrets, autorisant par exemple le VCS à rejeter leur enregistrement.

Ce RFC se focalise sur les secrets qui sont « au porteur » ("*bearer tokens*") c'est-à-dire que leur seule connaissance suffit à les utiliser ; aucune autre vérification n'est faite. Ce peut être un mot de passe, une clé d'API, etc. Voici un exemple avec une clé GitLab (je vous rassure, je l'ai révoquée depuis) :

La révélation de ces secrets via un enregistrement accidentel, par exemple dans un dépôt logiciel public, est un grand classique. Lisez par exemple le témoignage « "*I Published My AWS Secret Key to GitHub*" <https://www.dannyguo.com/blog/i-published-my-aws-secret-key-to-github/> », ou une aventure similaire, « "*Exposing your AWS access keys on Github can be extremely costly. A personal experience.*" <https://nagguru.medium.com/exposing-your-aws-access-keys-on-github-can-be-extremely
un avertissement de Github à ses utilisateurs <https://github.blog/2013-01-25-secrets-in-the-code/>, ou enfin une étude détaillée publiée à NDSS <https://www.ndss-symposium.org/ndss-paper/how-bad-can-it-git-characterizing-secret-leakage-in-public-github-repositories/>. Un `git add` de trop (ou bien un secret mis dans le code source) et, au prochain "*commit*", le secret se retrouve dans le dépôt, puis publié au premier `git push`.

L'idée de ce RFC est de marquer clairement ces secrets pour que, par exemple, des audits du dépôt les repèrent plus facilement. Ou pour que les systèmes d'intégration continue puissent les rejeter automatiquement.

Le plan d'URI est simple (section 2 du RFC) : la chaîne `secret-token:` suivie du secret. Un exemple serait `secret-token:E92FB7EB-D882-47A4-A265-A0B6135DC842%20foo` (notez l'échappement du caractère d'espacement). Par exemple avec les secrets au porteur pour HTTP du RFC 6750[1], cela donnerait un envoi au serveur :

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc6750.txt`

```
GET /authenticated/stuff HTTP/1.1
Host: www.example.com
Authorization: Bearer secret-token:E92FB7EB-D882-47A4-A265-A0B6135DC842%20foo
```

Le plan `secret-token:` est désormais dans le registre IANA <`https://www.iana.org/assignments/uri-schemes/uri-schemes.xml`>.

Je n'ai pas encore trouvé d'organisation qui distribue ces secrets au porteur en utilisant ce plan d'URI mais il semble que GitHub soit tenté.