

A3:2017-Sensitive Data Exposure



Fuite d'informations sensibles
dans la gestion de configuration

Informations
sensibles?

- Mot de passe
- Clé privée/Certificat

Et c'est une problème?



What Happened When I Leaked My Server Password on GitHub.com

June 10, 2020 By Craig Hays [Leave a Comment](#)

—

Reading Time: 7 minutes

I deployed a honeypot and 'accidentally' leaked a valid SSH username and password into a GitHub repository. This is what happened over the next 24 hours.

Retrieving secrets

Github dorks



Repositories	66K
Code	908K
Commits	85M+
Issues	3M
Discussions Beta	5K
Packages	511
Marketplace	66
Topics	352
Wikis	176K
Users	10K

[Advanced search](#) [Cheat sheet](#)

908,267 code results

Sort: Best match ▾

 ElrondNetwork/elrond-proxy-go
[cmd/proxy/config/walletKey.pem](#)

```
1  -----BEGIN PRIVATE KEY for
   8a2ee461bd72652fc33d8705b33cf240dc4a1531c5bf80bd4f4d92b6d83636ae-----
-
4  -----END PRIVATE KEY for
   8a2ee461bd72652fc33d8705b33cf240dc4a1531c5bf80bd4f4d92b6d83636ae-----
5  -----BEGIN PRIVATE KEY for
   e45b0dcd13663a6a21d9252882556966400d7940c4112e5b9d28d72aa1e853fd-----
```

Showing the top two matches Last indexed 19 days ago

 tamzi/mailler
[/google-oauth.pem](#)

```
3      localKeyID: 64 49 7D 65 20 31 34 33 33 32 35 11 39 35 87 99 39 33
4  Key Attributes: <No Attributes>
5  -----BEGIN RSA PRIVATE KEY-----
6  Put Your Private Key here{}Put Your Private Key here
7  Put Your Private Key here{}Put Your Private Key here
8  Put Your Private Key here{}Put Your Private Key here
```

Showing the top four matches Last indexed on Mar 24

<https://github.com/techgaun/github-dorks>

API

Exemple avec l'API Gitlab:

Récupérer tous les id des projets disponibles: **GET /projects**

Récupérer tous les id des commits de chaque projet: **GET
/projects/:id/repository/commits**

Récupérer le contenu du commit: **GET
/projects/:id/repository/commits/:sha/diff**

grep -i 'password|PRIVATE|...'

Comment s'en prémunir?

gitleaks

```
yvan@yvan-XPS-13-9360:~/tmp/gitleaks$ ~/go/bin/gitleaks -v --debug --branch=master --path=. --config-path=gitleaks.toml
INFO[0000] opening .
{
  "line": "    - password: 3P]Rw*~?MT",
  "lineNumber": 3,
  "offender": "password: 3P]Rw*~?MT",
  "offenderEntropy": -1,
  "commit": "c65b09b125abedc039231bac92611fd651ab02b1",
  "repo": ".",
  "repoURL": "",
  "leakURL": "",
  "rule": "Env Var",
  "commitMessage": "Initial commit\n",
  "author": "Cotonne",
  "email": "cotonne@users.noreply.github.com",
  "file": "config.yml",
  "date": "2021-05-10T13:57:23+02:00",
  "tags": ""
}
INFO[0000] scan time: 1 millisecond 814 microseconds
INFO[0000] commits scanned: 2
WARN[0000] leaks found: 1
```

Peut être ajouté à git hooks pre-commit

Génération de mot de passe à la volée

Exemple avec Kubernetes

```
apiVersion: v1
kind: Pod
metadata:
  name: secret-env-pod
spec:
  containers:
    - name: mycontainer
      image: redis
      env:
        - name: SECRET_USERNAME
          valueFrom:
            secretKeyRef:
              name: mysecret
              key: username
        - name: SECRET_PASSWORD
          valueFrom:
            secretKeyRef:
              name: mysecret
              key: password
      restartPolicy: Never
```