CVE-2021-43798 - Faille grafana présente en 8.X (2021)

Description

Grafana est un outil compatible avec Shinken pour créer des Dashboards pour un affichage avancé des courbes de métriques (*voir la page* Grafana - v8.3.2).

- Certaines versions de Grafana 8.X contiennent la faille suivante CVE-2021-43798
- Si vous avez installé Grafana, vous devez vérifier si votre version fait parti des version impactées (*voir ci-dessous*).

Résumé de la faille :

- Cette vulnérabilité permet à un attaquant non authentifié, de parcourir et récupérer des fichiers sur la machine (*Path Taversal*).
- Le chemin de l'URL vulnérable est : <grafana_host_url>/public/plugins/<"plugin-id"> où <"plugin-id"> est l'ID du plugin pour tout plugin installé.
- Chaque instance de Grafana est livrée avec des plugins pré-installés comme le plugin Prometheus ou le plugin MySQL de sorte que les URLs suivantes sont vulnérables pour chaque instance :
    - <grafana_host_url>/public/plugins/alertlist/
    - <grafana_host_url>/public/plugins/annolist/
    - <grafana_host_url>/public/plugins/barchart/
    - <grafana_host_url>/public/plugins/bargauge/
    - <grafana_host_url>/public/plugins/candlestick/
    - <grafana_host_url>/public/plugins/cloudwatch/
    - <grafana_host_url>/public/plugins/dashlist/
    - <grafana_host_url>/public/plugins/elasticsearch/
    - <grafana_host_url>/public/plugins/gauge/
    - <grafana_host_url>/public/plugins/geomap/
    - <grafana_host_url>/public/plugins/gettingstarted/
    - <grafana_host_url>/public/plugins/grafana-azure-monitor-datasource/
    - <grafana_host_url>/public/plugins/graph/
    - <grafana_host_url>/public/plugins/heatmap/
    - <grafana_host_url>/public/plugins/histogram/
    - <grafana_host_url>/public/plugins/influxdb/
    - <grafana_host_url>/public/plugins/jaeger/
    - <grafana_host_url>/public/plugins/logs/
    - <grafana_host_url>/public/plugins/loki/
    - <grafana_host_url>/public/plugins/mssql/
    - <grafana_host_url>/public/plugins/mysql/
    - <grafana_host_url>/public/plugins/news/
    - <grafana_host_url>/public/plugins/nodeGraph/
    - <grafana_host_url>/public/plugins/opentsdb
    - <grafana_host_url>/public/plugins/piechart/
    - <grafana_host_url>/public/plugins/pluginlist/
    - <grafana_host_url>/public/plugins/postgres/
    - <grafana_host_url>/public/plugins/prometheus/
    - <grafana_host_url>/public/plugins/stackdriver/
    - <grafana_host_url>/public/plugins/stat/
    - <grafana_host_url>/public/plugins/state-timeline/
    - <grafana_host_url>/public/plugins/status-history/
    - <grafana_host_url>/public/plugins/table/
    - <grafana_host_url>/public/plugins/table-old/
    - <grafana_host_url>/public/plugins/tempo/
    - <grafana_host_url>/public/plugins/testdata/
    - <grafana_host_url>/public/plugins/text/
    - <grafana_host_url>/public/plugins/timeseries/
    - <grafana_host_url>/public/plugins/welcome/
    - <grafana_host_url>/public/plugins/zipkin/

Pour détecter que l'on est vulnérable

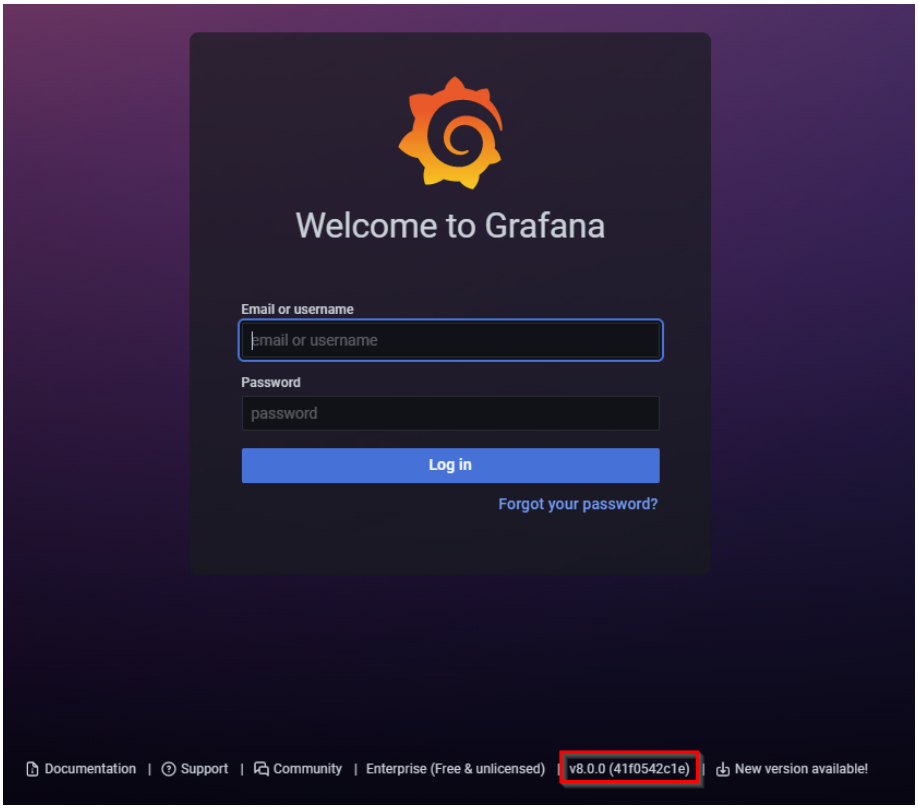
Les versions suivantes de Grafana comportent une failles de sécurité critique . Nous vous déconseillons de les installer :

- 8.0.0 à 8.0.6
- 8.1.0 à 8.1.7
- 8.2.0 à 8.2.6
- 8.3.0

La commande suivante permet d'afficher le numéro de version de Grafana :

```
/usr/sbin/grafana-cli -v
```

La version de Grafana apparaît aussi sur la page d'authentification :



Correction de la faille

Il faut que vous montiez faire une monté de version de Grafana vers la 8.3.2 (*voir la page* Grafana - v8.3.2).