Utilisation de Trivy pour le Scan de Sécurité de Grafana

Introduction

Trivy est un outil de scan de sécurité open-source développé par Aqua Security. Il est capable d'identifier les vulnérabilités dans des conteneurs Docker, des fichiers système, et d'autres environnements. Grafana, quant à lui, est une plateforme populaire pour la visualisation et la supervision des données. Dans ce compte rendu, nous montrons un exemple d'utilisation de Trivy pour scanner Grafana, en décrivant les étapes suivies ainsi que les résultats obtenus.

Présentation de Trivy

Trivy est un scanner rapide et simple d'utilisation qui analyse :
— Les conteneurs Docker.
— Les images conteneurisées.
— Les dépendances dans les fichiers `package.json`, `requirements.txt`, etc.
— Les configurations (Infrastructure as Code) telles que Kubernetes et Terraform.
Trivy détecte non seulement les vulnérabilités, mais fournit également des informations utiles sur leur gravité et les correctifs disponibles.

Exemple Pratique

Dans cet exemple, nous avons utilisé Trivy pour analyser l'image Docker de Grafana afin de détecter les vulnérabilités présentes.

Étapes Suivies

1. Installation de Trivy :
   L'installation a été effectuée en suivant les instructions officielles de Trivy disponibles sur leur site officiel (`https://aquasecurity.github.io/trivy/`).
2. Lancement du scan :
   La commande utilisée pour scanner l'image Docker de Grafana est la suivante :

   ```
   trivy image grafana/grafana
   ```

Résultats Obtenus

Le scan a permis de détecter plusieurs vulnérabilités dans l'image Docker de Grafana. Les résultats incluent :

— La liste des vulnérabilités classées par gravité : Critique, Haute, Moyenne, Faible.

— Des suggestions de mise à jour pour corriger certaines vulnérabilités.

Voici les captures d'écran des résultats obtenus :

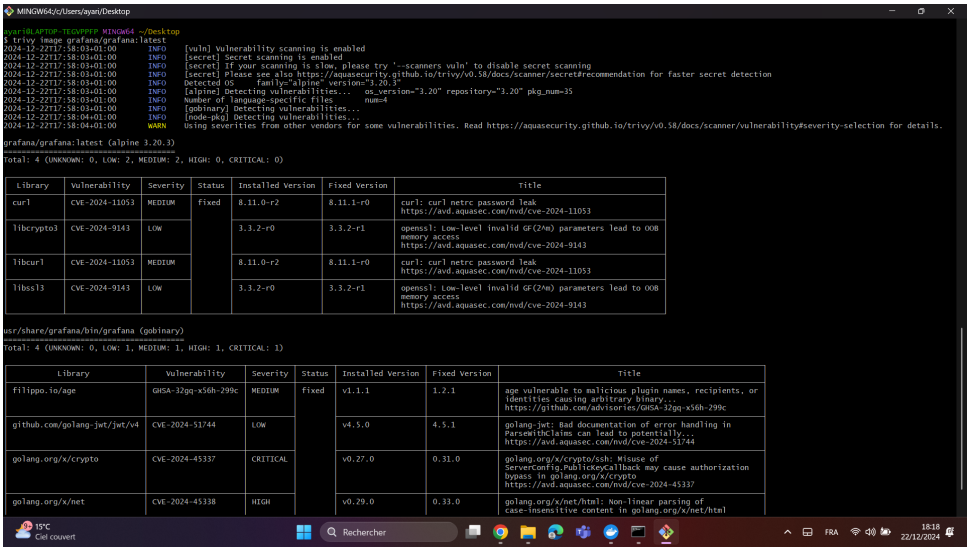

FIGURE 1 – Résultats du scan montrant les vulnérabilités détectées.

Conclusion

L'analyse de sécurité avec Trivy est essentielle pour détecter et corriger les vulnérabilités dans les conteneurs Docker et autres environnements. Dans cet exemple, le scan de Grafana a permis d'identifier des problèmes critiques et de fournir des pistes pour les résoudre. Cela souligne l'importance d'intégrer des outils de sécurité comme Trivy dans le cycle de vie de développement des applications pour garantir leur robustesse.