Proposition de stage sur la reproduction de vulnérabilités logicielles

Olivier Levillain

CVE et reproduction de vulnérabilités

CVE

- Base de données des vulnérabiltés logicielles
- Métadonnées de qualité variable
- Identifier la cible d'une faille est complexe (CPE)

CVE et reproduction de vulnérabilités

CVE

- Base de données des vulnérabiltés logicielles
- Métadonnées de qualité variable
- Identifier la cible d'une faille est complexe (CPE)

Pourquoi reproduire les vulnérabilités

- Mieux comprendre la menace de manière concrète
- Valider des outils de sécurité
- Former et entraîner

VauCanSSon et DECRET

VauCanSSon

- 2022-2023 : Commande d'Orange pour évaluer leur outil SNAPPY/Onager
- Étude d'un corpus de vulnérabilités affectant Linux
- Restriction du périmètre aux programmes *userland* sur des serveurs

VauCanSSon et DECRET

VauCanSSon

- 2022-2023 : Commande d'Orange pour évaluer leur outil SNAPPY/Onager
- Étude d'un corpus de vulnérabilités affectant Linux
- Restriction du périmètre aux programmes *userland* sur des serveurs

DECRET

- Outil de reproduction (semi-)automatisée de vulnérabilités dans Debian
- Présentation au SSTIC en 2023
- (l'auteur est dans la salle)

Limites actuelles et objectifs du stage

Limites actuelles

- Métadonnées parfois de piètre qualité
- Absence de code d'exploitation pour valider la reproduction
- Dépendance de la reproductibilité à divers paramètres
  - par exemple pour les corruptions mémoire

Limites actuelles et objectifs du stage

Limites actuelles

- Métadonnées parfois de piètre qualité
- Absence de code d'exploitation pour valider la reproduction
- Dépendance de la reproductibilité à divers paramètres
  - par exemple pour les corruptions mémoire

Proposition de stage

- Reproduire des vulnérabilités dans Nix (OS)
  - apports de l'aspect immuable/reproductible
- Comment garantir la capacité à reproduire les vulnérabilités
  - quelles sont les métadonnées nécessaires ?
  - application à Debian et Nix
  - jusqu'à quand peut-on remonter ?

Candidatures ?

Si vous cherchez un stage orienté recherche sur un tel sujet, venez me parler !

Stage co-encadré par Julien Malka (doctorant à TP)