Reproduction automatisée de vulnérabilités logicielles dans un environnement conteneurisé

DECRET : DEbian Cve REproducer Tool

Clément Parssegny, Olivier Levillain, Maxime Belair, Mathieu Bacou, Gaël Thomas
ANSSI, Laboratoire SAMOVAR - Télécom SudParis/IP Paris, Orange

09 Juin 2023

Contexte et motivations

Objectif initial

Projet d'évaluation d'un outil permettant d'ajouter dynamiquement des politiques de sécurité (SNAPPY[1]).

$\Rightarrow$ Nécessité d'avoir des conteneurs vulnérables pour tester l'efficacité des politiques de sécurité.

1. **Maxime Bélair, Sylvie Laniepce et Jean-Marc Menaud. "SNAPPY : Programmable Kernel-Level Policies for Containers". In : SAC '21.**

Contexte et motivations

Difficultés rencontrées

- Identification de la version vulnérable
- Disponibilité de la version vulnérable
- Dépendances logicielles

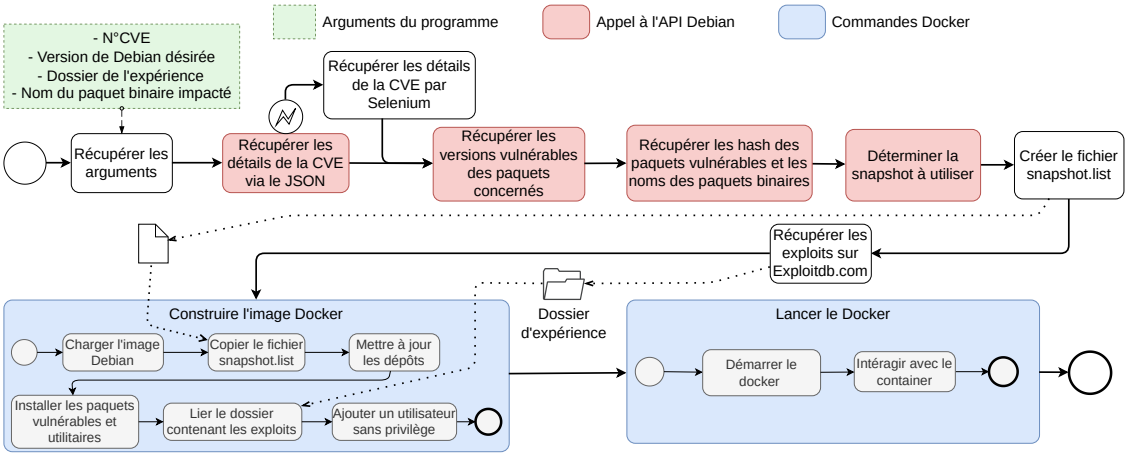
Cahier des charges : générateur d'images Docker Debian vulnérables à une CVE donnée

- Pas de solution automatisée connue
- Choix retenu : utiliser les paquets binaires de Debian

Pourquoi Debian ?

- Distribution largement utilisée couvrant un grand nombre de packages Linux
- Métadonnées des vulnérabilités disponibles (*Debian Security Advisories*)
- *Snapshots* réguliers des dépôts (toutes les 6h) depuis 2005

Fonctionnement d'une exécution de l'outil



Fonctionnement d'une exécution de l'outil : détails de la vulnérabilité

Le *Security Bug Tracker* de Debian fournit un JSON qui énumère les CVE et leurs détails

Entrée

```
CVE-2017-5932
```

Sortie

```
[{'src_package': 'bash',
  'release': 'bullseye',
  'fixed_version': '4.4-3'}]
```

Fonctionnement d'une exécution de l'outil : version vulnérable

API Debian [2]

Entrée

```
[{'src_package': 'bash',
  'fixed_version': '4.4-3'}]
```

Sortie

```
[{'src_package': 'bash',
  'fixed_version': '4.4-3',
  'vuln_version': '4.4-2'}]
```

2. https://salsa.debian.org/snapshot-team/snapshot/raw/master/API

Fonctionnement d'une exécution de l'outil : hash de la source et binaire associé

API Debian

Entrée

```
[{'src_package': 'bash',
  'vuln_version': '4.4-2'}]
```

Sortie

```
[{'hash': 'dcda82bf261ec6ce1c4429932d4e8280c05e9d8c',
  'bin_name': ['bash']}]
```

Fonctionnement d'une exécution de l'outil : identifiant du timestamp

API Debian

Entrée

```
[{'hash': 'dcda82bf261ec6ce1c4429932d4e8280c05e9d8c'}]
```

Sortie

```
[{'first_seen': '20161116T035853Z'}]
```

Ecriture du fichier .list pour apt

- `http://snapshot.debian.org/archive/debian/20161116T035853Z/ unstable main`

Fonctionnement d'une exécution de l'outil : preuves de concept

- Utilisation d'exploit-db.com pour récupérer le contenu des PoC.

Construction du conteneur

1. Image Debian
2. Copie du fichier source construit
3. Copie des PoC
4. Mise à jour des dépôts
5. Installation des paquets vulnérables
6. Ajout d'un utilisateur non-administrateur

Démonstration

- CVE-2017-5932 : exécution de commandes via la complétion bash

Avantages et limites

Avantages

- Installation de versions vulnérables facilitée
- Possibilité de tester des PoC publics
- Couverture générale de l'écosystème Linux

Limites

- Pas de DSA, pas de résultat !
- Pas de reproduction de failles noyau
- Manque de PoC publics
- Isolation limitée (Attention aux sorties de Docker !)

Résultats

Objectif principal rempli

DECRET utilisé pour aider à l'évaluation de SNAPPY

Perspectives

- Recherche : étudier les traces laissées par un exploit, évaluer des outils de détection
- Enseignement : illustrer des concepts de programmation sécurisée [3]
- Administration système : évaluer une configuration de serveur utilisant un paquet vulnérable

3. **utilisation envisagée en travaux pratiques à Télécom SudParis**

Conclusion

DECRET : vous pouvez aider !

- https://github.com/Orange-OpenSource/decret
- Retours sur expérience et contributions bienvenus

Contact : clement.parssegny@ssi.gouv.fr