Exercice
A08:2021 Manque d'intégrité des données et du logiciel

Le **manque d'intégrité des données et des logiciels** se produit lorsque les logiciels, mises à jour ou données importantes ne sont pas bien protégés contre les modifications ou les piratages. Cela peut se produire si :

- L'utilisation de plugins ou de bibliothèques provenant de sources non fiables.
- Des pipelines CI/CD insuffisamment sécurisés.
- Des mises à jour logicielles appliquées sans vérification d'intégrité adéquates.
- La désérialisation de données non sécurisées, ce qui peut permettre des attaques.

Exemples :

1. **Mises à jour sans signature** : de nombreux appareils, comme les routeurs, n'ont pas de mécanisme pour vérifier l'authenticité des mises à jour.
2. **Attaque SolarWinds** : les mécanismes de mise à jour compromis ont permis la distribution de logiciels malveillants à des milliers d'organisations.
3. **Données sérialisées vulnérables** : des attaquants peuvent exploiter des données sérialisées non sécurisées pour prendre le contrôle d'un système.

Mesures de protection :

- Utiliser des signatures numériques pour vérifier l'intégrité des données et des logiciels.
- S'assurer que les dépendances logicielles proviennent de sources fiables.
- Héberger des dépôts internes approuvés pour les organisations à haut risque.
- Vérifier régulièrement les composants avec des outils comme OWASP Dependency Check.
- Contrôler strictement l'accès et la configuration des pipelines CI/CD.