# Pourquoi les chaînes d'approvisionnement se font-elles pirater ?

En l'absence de mesures automatisées de sécurité supervisant le cycle DevOps, il est facile pour des développeurs déjà très sollicités d'introduire par accident du code malveillant, des problèmes de conformité ou des violations de sécurité dans leur code. Voici cinq chiffres qui montrent l'étendue du problème et expliquent comment l'empêcher de s'infiltrer dans vos logiciels.

## Vulnérabilités non corrigées

### PLUS DE 16,000

**Nombre de nouvelles vulnérabilités signalées** au National Institute of Standards et au Technology NIST et analysées par ces instances en 2023.
(avant juillet - https://nvd.nist.gov/general/nvd-dashboard)

### 2,548

**de ces vulnérabilités ont reçu la notation Critique.** La plupart d'entre elles sont exploitables en passant par le réseau, ne requièrent pas de privilèges utilisateur particuliers ni d'interactions spécifiques, avec un niveau de complexité d'attaque très bas.

La solution passe par une analyse persistante de la totalité du code source et des bibliothèques, réalisée par un système ayant accès à une base de données complète des vulnérabilités documentées.

## Secrets exposés

### 1 MILLIARD

**Nombre d'enregistrements à caractère personnel compromis** lors de la plus grande violation de données jamais observées, déclenchée par la divulgation d'un secret. (https://securityboulevard.com/2022/07/the-worlds-largest-breach-root-cause-secrets-in-code/)
Le code publié sur un blog du réseau chinois de développeurs logiciels (Chinese Software Developer Networks, CSDN), «contenait des identifiants d'accès en texte brut consultables par tout le monde».

Les enregistrements mis en vente sur le dark web renfermaient des «noms, adresses, identifiants nationaux, casiers judiciaires et dossiers médicaux provenant d'un pays d'Asie».

Lorsqu'une erreur d'inattention expose des secrets, les conséquences sont catastrophiques : compromission de données confidentielles de l'entreprise ou d'actifs de type code source, voire compromission de l'ensemble du système de développement lui-même.

On trouve facilement de nombreuses statistiques alarmantes à ce sujet. À la suite d'une analyse de données réalisée par son équipe de Threat Intelligence, Unit 42, Palo Alto Networks rapporte les faits suivants:

**83%**
des organisations possèdent des identifiants codés en dur dans leurs systèmes de gestion du code

**75%**
des organisations possèdent des instances de VM avec des ports non-HTTP connectées à Internet.

**55%**
des organisations n'appliquent pas le chiffrement de volume AWS EBS.

https://start.paloaltonetworks.com/unit-42-cloud-threat-report-volume-7

Les procédures par lesquelles les développeurs exposent des secrets par accident sont connues: un outil d'analyse intelligent est capable de scanner le code source pour y rechercher ces problèmes et les signaler avant qu'ils ne causent du tort à l'entreprise.

## Productivité DevSecOps

### 6,7 M$

**Valeur des gains d'efficacité opérationnelle** dégagés grâce à l'automatisation des flux de gestion des vulnérabilités et de la conformité sur les ressources open source, d'après une étude Forrester Consulting commanditée par JFrog «Total Economic Impact™ de la plateforme JFrog».
(https://jfrog.com/tei/)

L'étude Forrester explique que l'automatisation de ces processus a entraîné une accélération de la livraison des logiciels, une amélioration de l'efficacité opérationnelle et de la productivité, ainsi qu'une réduction des coûts de gestion liés à l'ingénierie cloud.

Dans les systèmes DevOps conventionnels, la productivité est freinée par la disparité des processus utilisés pour contrôler les problèmes liés aux vulnérabilités et à la conformité. L'automatisation de ces contrôles relance la productivité sur l'ensemble du cycle de développement en libérant les développeurs.

Le retour sur investissement a été estimé à **393%**

## Le coût d'une absence de DevSecOps

### 4,45 M$

**Coût total moyen d'une violation de données en 2023,** selon le Rapport IBM 2023 sur le coût d'une violation de données.
(https://www.ibm.com/reports/data-breach)

L'entreprise est allée très loin en mesurant l'impact (positif ou négatif) de 27 facteurs différents sur le coût d'une violation de données.

Les plus grandes économies

**(249,278 $)**

découlent d'une approche DevSecOps.

Elle a ensuite mesuré l'impact subi par les entreprises présentant le niveau d'adoption du DevSecOps le plus élevé, en le comparant à celles dont le niveau d'adoption DevSecOps était le plus faible.

Les économies réalisées par les entreprises possédant une forte culture DevSecOps s'élèvent à

**1,68 M$**

soit

**34%**
de moins que les entreprises négligeant cette approche.

Lorsqu'une violation de données se produit, c'est que quelqu'un a commis une erreur, et les erreurs de sécurisation des logiciels se trouvent tout en haut de la liste. Tous les efforts que vous déployez pour renforcer l'efficacité de la sécurité des logiciels contribueront à réduire le risque de violation.

## Curation Open-Source

### 9,074,000

**Nombre de versions logicielles créées dans les 12 mois antérieurs** au 3 juillet 2023 dans npm, le célèbre gestionnaire de package open source pour code JavaScript, utilisé par les développeurs du monde entier.
(https://blog.sandworm.dev/state-of-npm-2023-the-overview#-heading-packages-created-per-month)



Et on ne parle là que des nouvelles versions. Plus de 3,3 millions de packages sont actuellement disponibles sur npm, ce qui n'aide pas les développeurs à déterminer ceux qui sont sûrs, ou même ceux qui font réellement ce qu'ils prétendent faire.

La solution? Fournir aux développeurs une présélection de bibliothèques, dont l'absence de problème de sécurité dans le code a été validée. Et même dans ce cas, le cycle DevOps ne doit pas s'affranchir d'une analyse rigoureuse du code pour y rechercher les vulnérabilités connues et inconnues. Cette démarche permet non seulement de gagner du temps, mais aussi d'éviter les dépenses inutiles engagées pour corriger les vulnérabilités importées dans la base de code. Par ailleurs, assurez-vous de tenir à disposition du directeur de la sécurité ou autre personne responsable une liste à jour des importations.

## Références


- **National Vulnerability Database Dashboard:** https://nvd.nist.gov/general/nvd-dashboard
- **The World's Largest Breach. Root cause: Secrets in Code (Security Boulevard):** https://securityboulevard.com/2022/07/the-worlds-largest-breach-root-cause-secrets-in-code/
- **Palo Alto Networks Unit 42 Cloud Threat Report, Volume 7:** https://start.paloaltonetworks.com/unit-42-cloud-threat-report-volume-7
- **Forrester Consulting Report - Total Economic ImpactTM of the JFrog Software Supply Chain Platform:** https://jfrog.com/tei/
- **IBM - Cost of a Data Breach Report 2023:** https://www.ibm.com/reports/data-breach
- **State of Npm 2023 - Packages Created Per Month (Sandworm blog):** https://blog.sandworm.dev/state-of-npm-2023-the-overview#heading-packages-created-per-month



DARKReading

Sponsorisé par JFrog