Flux d’informations de Kaspersky sur les menaces liées aux logiciels open source

kaspersky prêts pour l’avenir

Attaques contre la chaîne d'approvisionnement en logiciels

Dans ce type d'attaque, les cybercriminels compromettent les systèmes ou les outils de développement logiciels d'un fournisseur de logiciels en intégrant du code malveillant ou un programme malveillant aux logiciels avant qu'ils ne soient distribués aux clients.

Flux d'informations de Kaspersky sur les menaces liées aux logiciels open source

Les cybermenaces évoluent constamment et deviennent de plus en plus sophistiquées, ce qui complique la protection des entreprises. Le flux d'informations de Kaspersky sur les menaces liées aux logiciels open source fournit des informations à jour sur les menaces et les vulnérabilités, permettant aux entreprises de protéger leurs réseaux, leurs terminaux et leurs données critiques. Le flux d'informations de Kaspersky sur les menaces liées aux logiciels open source est conçu pour être inclus dans les processus DevSecOps pour surveiller les composants open source utilisés dans le développement afin de détecter les menaces cachées.

Une nouvelle approche de la sécurité

La plupart des développeurs de logiciels incluent des logiciels open source dans leur cycle de développement et ont tendance à faire confiance à l'intégrité de ces paquets.

Alors que le nombre et la gravité des cybermenaces ne cessent d'augmenter, la méthodologie classique DevOps de développement de logiciels a commencé à évoluer vers une approche plus soucieuse de la sécurité, connue sous le nom de DevSecOps. Cette approche préconise la mise en œuvre de pratiques de sécurité depuis les phases initiales de planification et de conception jusqu'au développement, aux tests et au-delà. Cet état d'esprit doit également s'appliquer à tous les logiciels open source utilisés dans le cycle de développement.

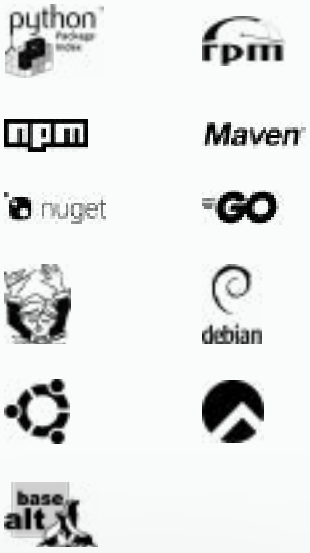
Kaspersky a conçu un flux de données précieux pour permettre d'appliquer cette approche de la sécurité aux logiciels open source : Flux d'informations de Kaspersky sur les menaces liées aux logiciels open source. Il s'agit d'un ensemble de données textuelles sans binaire, qui révèle les menaces et les vulnérabilités au sein de tous les paquets open source connus.

Types de menaces

Le flux d'informations de Kaspersky sur les menaces liées aux logiciels open source couvre les types de menaces suivants :

- Paquets compromis avec des fonctionnalités altérées dans certaines régions
- Paquets contenant des logiciels potentiellement dangereux comme des mineurs de cryptomonnaies, des outils de piratage, etc.
- Paquets compromis contenant des messages politiques
- Paquets présentant des vulnérabilités
- Paquets de logiciels présentant du code malveillant

Gestionnaires de paquets



Avis de vulnérabilité

Contenu du flux

Gestionnaires de paquets

Le flux fournit des informations sur les paquets à partir des gestionnaires de paquets suivants*, dont les stockages sont régulièrement analysés :
Pypi, Npm, NuGet, Maven, Composer, Go, Rpm, Debian.

Avis de vulnérabilité

Tous les paquets de tous les stockages sont automatiquement comparés aux avis de vulnérabilité suivants : Avis de sécurité GitHub, CVE MITRE, avis de sécurité Debian, alertes de sécurité CentOS, avis de sécurité RedHat (seuls les liens croisés vers cet avis sont fournis).

Contexte

En plus de la liste des paquets, le contexte utile suivant est également fourni :

Pour les vulnérabilités :

- Connexion à l'écosystème
- Impact sur le système
- Liste des versions vulnérables
- Versions vulnérables CPE/PURL pour l'automatisation
- Listes des versions recommandées dont les vulnérabilités ont été corrigées
- Prise en charge des versions du système d'exploitation (pour les paquets *nix)
- Liens croisés vers les avis de vulnérabilité
- Hachages des exploits actuellement utilisés in the wild (ITW)

Pour les paquets malveillants et compromis :

- Connexion à l'écosystème
- Impact sur le système : programmes malveillants, outil de piratage, autre
- Niveau de gravité
- Versions compromises des paquets
- Hachages des versions compromises des paquets
- CWE (Common Weakness Enumeration) : pour l'instant, uniquement pour les paquets de programmes malveillants

Valeur commerciale

Fournit une valeur commerciale significative aux entreprises en leur permettant de :

Détection des menaces avancées

Fournir une intelligence en temps réel sur les dernières cybermenaces et vulnérabilités liées aux logiciels open source. Les entreprises peuvent ainsi améliorer leurs capacités de détection des menaces et repérer les attaques potentielles avant qu'elles ne fassent des dégâts.

Améliorer la réponse aux incidents

Fournir des informations précieuses pour aider les entreprises à réagir rapidement et efficacement à la menace. Cela peut contribuer à minimiser l'impact de l'incident et à réduire le temps et les ressources nécessaires à la réponse aux incidents.

Renforcer la posture de sécurité

Aider les entreprises à se tenir informées des dernières menaces et vulnérabilités en matière de sécurité liées aux logiciels open source qu'elles utilisent. Ces informations peuvent aider les entreprises à identifier les vulnérabilités et à y remédier en temps utile, ce qui réduit le risque d'exploitation de ces vulnérabilités par les cybercriminels.

Réduire les risques de sécurité

Aider les entreprises à réduire les risques de sécurité liés à l'utilisation de logiciels open source. Cela peut contribuer à protéger les données critiques, la propriété intellectuelle et la réputation de l'entreprise.

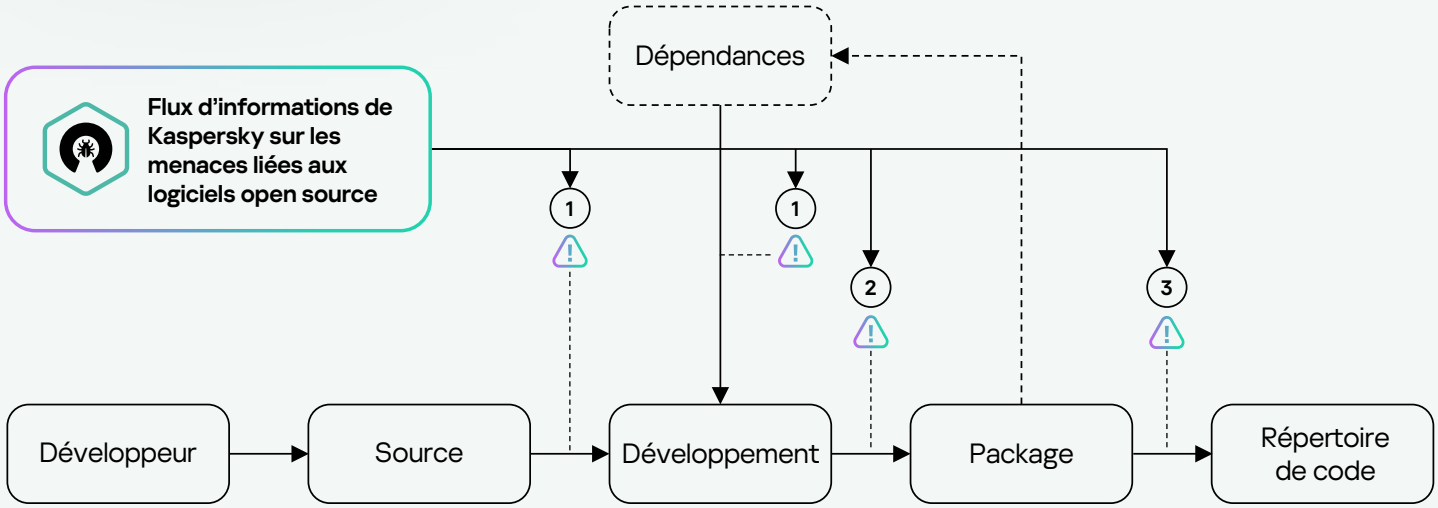
Gagner du temps et de l'argent

Fournir aux entreprises un moyen rentable et efficace de se tenir informées des dernières menaces et vulnérabilités en matière de sécurité liées aux logiciels open source. Les entreprises peuvent ainsi économiser du temps et de l'argent sur le développement et la maintenance de leurs propres systèmes de Threat Intelligence.

Le flux est livré au format JSON

Cas d'utilisation

Le cas d'utilisation recommandé pour le flux d'informations de Kaspersky sur les menaces liées aux logiciels open source est le suivant : faire correspondre l'identifiant des paquets du flux avec les paquets utilisés dans le développement sur la base d'un ou plusieurs paramètres, comme le nom du paquet, la version du paquet, etc.



Points d'intégration

1

Au stade du téléchargement de paquets à partir de stockages par un développeur open source (point d'intégration – stockage proxy).

2

Au stade de la compilation par le développeur du code source, y compris en vérifiant les paquets dépendants, qui peuvent également poser problème (point d'intégration – chaîne de montage).

3

Au stade de la publication du code source dans le stockage (point d'intégration – mécanisme de publication)

La recommandation en cas de détection d'un paquet problématique est d'agir conformément à la stratégie adoptée par l'entreprise (notification au développeur, traitement du risque, blocage, etc.)

Kaspersky Threat Intelligence

En savoir plus

www.kaspersky.fr

#kaspersky
#bringonthefuture