Kaspersky Open Source Software Threats Data Feed

kaspersky preparados para el futuro

Ataques a la cadena de suministro de software

En este tipo de ataque, los ciberdelincuentes ponen en riesgo los sistemas o las herramientas de desarrollo de software de un proveedor, e insertan malware o código malicioso en el software antes de que se distribuya a los clientes.

Kaspersky Open Source Software Threats Data Feed

Las ciberamenazas evolucionan constantemente y son cada vez más sofisticadas, lo que dificulta la protección de las empresas. Kaspersky Open Source Software Threats Data Feed proporciona información actualizada sobre amenazas y vulnerabilidades, permitiendo a las empresas proteger sus redes, endpoints y datos críticos. Además, está diseñada para incluirse en los procesos de DevSecOps para la supervisión de los componentes de código abierto usados en el desarrollo con el fin de detectar las amenazas ocultas.

Un nuevo enfoque de seguridad

La mayoría de los desarrolladores de software incluyen paquetes de software de código abierto en su ciclo de desarrollo y tienden a confiar en la integridad de estos paquetes.

A medida que el número y la gravedad de las ciberamenazas siguen aumentando, la metodología clásica de DevOps de desarrollo de software empieza a cambiar hacia un enfoque más centrado en la seguridad, conocido como DevSecOps. Este enfoque consiste en implementar prácticas de seguridad desde las etapas iniciales de planificación y diseño, hasta el desarrollo, las pruebas y las etapas posteriores. Adicionalmente, debe aplicarse a todo software de código abierto que se use en el ciclo de desarrollo.

Kaspersky ha diseñado una valiosa fuente de datos para ayudar a aplicar este enfoque de seguridad a los programas de código abierto: Kaspersky Open Source Software Threats Data Feed. Se trata de un conjunto de datos sin binarios y solo en texto que revela las amenazas y vulnerabilidades en cada paquete de código abierto conocido.

Tipos de amenazas

Kaspersky Open Source Software Threats Data Feed cubre los siguientes tipos de amenazas:

Paquetes en riesgo con funcionalidad modificada en determinadas regiones

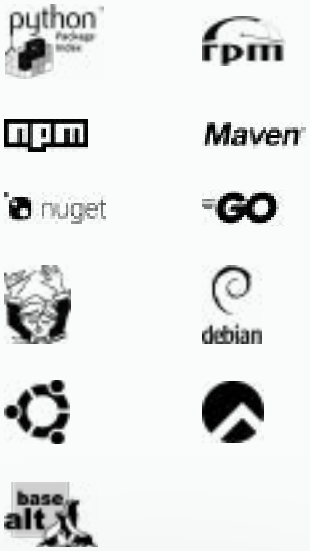
Paquetes que contienen software potencialmente peligroso, como criptomineros, herramientas de piratería informática, etc.

Paquetes en riesgo que contienen mensajes políticos

Paquetes con vulnerabilidades

Paquetes con código malicioso

Administradores de paquetes



Avisos de vulnerabilidad

Contenido de la fuente

Administradores de paquetes

La fuente proporciona información sobre paquetes de los siguientes administradores de paquetes*, cuyos repositorios se analizan con regularidad: Pypi, Npm, NuGet, Maven, Composer, Go, Rpm, Debian.

Avisos de vulnerabilidad

Todos los paquetes de todos los repositorios se comparan automáticamente con los siguientes avisos de vulnerabilidad: GitHub Security Advisory, CVE MITRE, Debian, Security Advisory, CentOS Security Alerts, RedHat Security Advisory (solo se proporcionan vínculos cruzados a estos avisos).

Contexto:

Junto con la lista de paquetes, también se proporciona el siguiente contexto útil:

En caso de vulnerabilidades:

- Conexión con el ecosistema
- Impacto en el sistema
- Lista de versiones vulnerables
- Versiones vulnerables de CPE / PURL para automatización
- Listas de versiones recomendadas con vulnerabilidades con parches
- Compatibilidad con versiones del sistema operativo (para paquetes *nix)
- Vínculos cruzados a los avisos de vulnerabilidad
- Hashes de exploits usados actualmente en circulación

En caso de paquetes maliciososy en riesgo:

- Conexión con el ecosistema
- Impacto en el sistema: malware, hacktool, otros
- Gravedad
- Versiones de paquetes en riesgo
- Hashes de versiones de paquetes en riesgo
- CWE (Enumeración de debilidades comunes): por el momento, solo para paquetes de malware

Valor Comercial

Proporciona un importante valor empresarial a las organizaciones ya que les permite lo siguiente:

Mejora la detección de amenazas

Proporciona información de inteligencia en tiempo real sobre las últimas ciberamenazas y vulnerabilidades relacionadas con el software de código abierto. Esto permite a las organizaciones mejorar sus capacidades de detección de amenazas y detectar ataques potenciales antes de que puedan causar daños.

Mejora la respuesta a incidentes

Proporciona información valiosa para ayudar a las organizaciones a responder rápida y eficazmente a la amenaza. Esto puede ayudar a minimizar el impacto del incidente y reducir el tiempo y los recursos necesarios para la respuesta a este.

Fortalece el plan de seguridad

Ayuda a las organizaciones a mantenerse informadas sobre las últimas amenazas a la seguridad y las vulnerabilidades relacionadas con el software de código abierto que usan. Esta información puede ayudar a las organizaciones a identificar y corregir las vulnerabilidades a tiempo, lo que reduce el riesgo de aprovechamiento por parte de los ciberdelincuentes.

Reduce los riesgos de seguridad

Ayuda a las organizaciones a reducir los riesgos de seguridad asociados al uso de software de código abierto. Esto puede ayudar a proteger los datos críticos, la propiedad intelectual y la reputación de la organización.

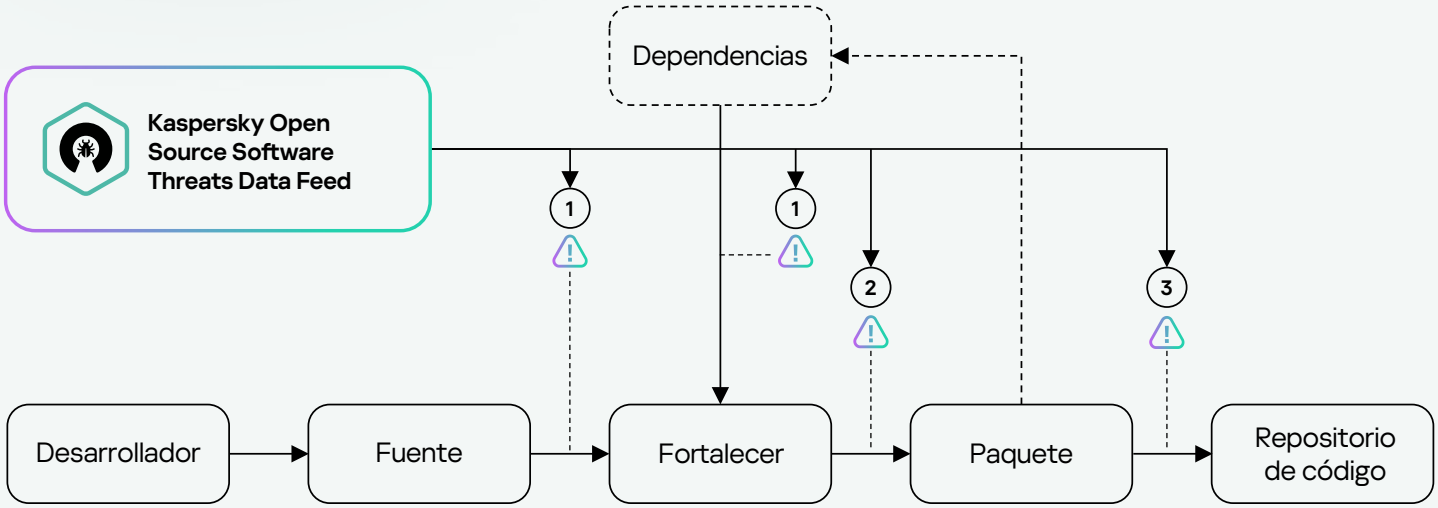
Ahorra tiempo y dinero

Proporciona a las organizaciones una forma rentable y eficaz de mantenerse informadas sobre las últimas amenazas a la seguridad y las vulnerabilidades relacionadas con el software de código abierto. Esto puede ayudar a las organizaciones a ahorrar tiempo y dinero en la creación y el mantenimiento de sus propios sistemas de inteligencia de amenazas.

La fuente se proporciona en formato JSON

Casos de uso

El caso de uso recomendado para Kaspersky Open Source Software Threats Data Feed es el siguiente: comparar el identificador de paquetes de la fuente con los paquetes usados en el desarrollo en función de uno o varios parámetros, como el nombre del paquete, la versión del paquete, etc.



Puntos de integración

1

En la etapa de descarga de paquetes desde los repositorios por parte de un desarrollador de código abierto (punto de integración: repositorio proxy).

2

Durante la etapa de compilación del código fuente por el desarrollador, asegúrese de verificar los paquetes dependientes, ya que también pueden ser problemáticos (punto de integración: línea de montaje).

3

En la etapa de publicación del código fuente en el repositorio (punto de integración: mecanismo de publicación).

La recomendación al detectar un paquete problemático es actuar según la política de la organización (notificación al desarrollador, gestión de riesgos, bloqueo, etc.).

Kaspersky Threat Intelligence

Conozca más

https://latam.kaspersky.com

#kaspersky
#bringonthefuture