Kaspersky Open Source Software Threats Data Feed

kaspersky активируй будущее

Атаки на цепочки поставок

ПО с открытым исходным кодом часто содержит серьёзные уязвимости и специально скрытые угрозы, которые могут скомпрометировать продукты, использующие это ПО.

Kaspersky Open Source Software Threats Data Feed

Киберугрозы постоянно развиваются и становятся всё более сложными, что затрудняет защиту бизнеса. Kaspersky Open Source Software Threats Data Feed предоставляет актуальную информацию об угрозах и уязвимостях, позволяя компаниям-разработчикам программного обеспечения своевременно обнаружить попытку или факт использования в своем коде опасных open source пакетов и принять соответствующие меры. Kaspersky Open Source Software Threats Data Feed разработан для включения в процессы DevSecOps и позволяет осуществлять мониторинг использования пакетов с открытым исходным кодом с целью обнаружения скрытых угроз.

Новый подход к безопасности

Большинство разработчиков программного обеспечения включают пакеты с открытым исходным кодом в свои разработки и обычно доверяют функциональности и целостности этих пакетов.

Количество, сложность киберугроз и ущерб от них продолжают расти, классическая методология DevOps разработки ПО начала смещаться в сторону более продуманного подхода к безопасности, известного как DevSecOps. Данный подход предлагает концентрировать внимание на введении практик безопасности с самого начала – от планирования и проектирования до разработки, тестирования и дальнейшего развития программного продукта. Эту методологию целесообразно применять и ко всему открытому ПО, используемому в цикле разработки.

«Лаборатория Касперского» организовала подписку на данные об угрозах Kaspersky Open Source Software Threats Data Feed, которая поможет на практике применять данный подход к безопасности в отношении программного обеспечения с открытым исходным кодом.

Типы угроз

Kaspersky Open Source Software Threats Data Feed предоставляет информацию о следующих типах угроз:

Скомпрометированные пакеты, меняющие функциональность в зависимости от региона

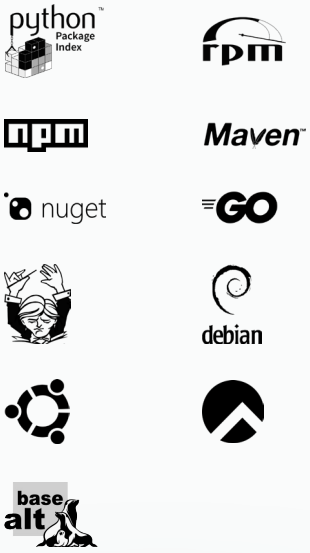
Пакеты с небезопасным ПО, в том числе крипто-майнерами, хакерскими инструментами и т.д.

Скомпрометированные пакеты, демонстрирующие политические лозунги

Пакеты, содержащие уязвимости

Пакеты, содержащие вредоносный код

Пакетные менеджеры



Реестры уязвимостей

Состав

Пакетные менеджеры

Сервис предоставляет информацию о пакетах для следующих пакетных менеджеров*: Pypi, Npm, NuGet, Maven, Composer, Go, Rpm, Debian, Alt Linux, Ubuntu, Rocky Linux.

Уязвимости

Все пакеты из указанных репозиториев автоматически и регулярно проверяются по следующим реестрам уязвимостей: GitHub Security Advisory, CVE MITRE, Debian Security Advisory, CentOS Security Alerts, RedHat Security Advisory (на этот реестр предоставляются только кросс-ссылки).

Дополнительный контекст

Дополнительно к списку пакетов предоставляется следующий полезный контекст:

Касательно уязвимостей:

- Связь с экосистемой
- Влияние на систему (импакт)
- Списки уязвимых версий
- CPE/PURL уязвимых версий (для автоматизации)
- Списки рекомендованных версий с исправленными уязвимостями
- Применимость к версиям ОС (для *nix-пакетов)
- Кросс-ссылки на бюллетени безопасности
- Хэши актуальных и используемых эксплойтов

Касательно вредоносных и скомпрометированных пакетов:

- Связь с экосистемой
- Влияние на систему (импакт): malware, hacktool, other
- Серьезность проблемы (severity)
- Скомпрометированные версии пакетов
- Хэши скомпрометированных версий пакетов
- CWE (Common Weakness Enumeration) на текущий момент только на malware-пакетах

Ценность для бизнеса

Проактивное обнаружение угроз

Сервис предоставляет оперативную информацию о последних киберугрозах и уязвимостях, связанных с ПО с открытым исходным кодом. Это позволяет компаниям увеличить возможность обнаружения угроз и выявлять потенциальные атаки до того, как они смогут нанести ущерб.

Снижение рисков безопасности

Сервис помогает снизить риски безопасности, связанные с использованием программного обеспечения с открытым исходным кодом. Это помогает защитить важные данные организации, интеллектуальную собственность и репутацию.

Экономия ресурсов

Сервис предоставляет экономичный и действенный способ быть в курсе последних угроз безопасности и уязвимостей, связанных с программным обеспечением с открытым исходным кодом. Это помогает компаниям сэкономить время и деньги на создании и обслуживании собственных систем анализа угроз.

Улучшенный процесс реагирования на инциденты

Сервис предоставляет ценную информацию, которая дает компаниям возможность быстро и эффективно реагировать на угрозу. Это помогает свести к минимуму влияние инцидента и сократить время и ресурсы, необходимые для реагирования на него.

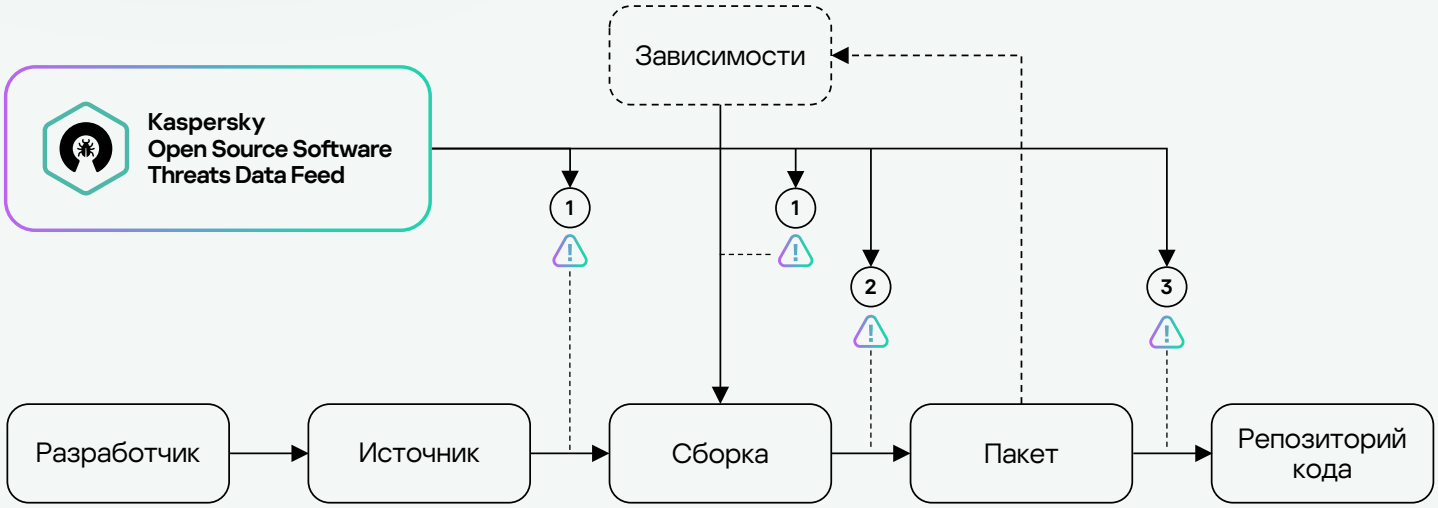
* Настоящий список может пополняться другими популярными репозиториями

Сервис предоставляет данные в формате JSON

Сценарии использования

Рекомендованный сценарий использования Kaspersky Open Source Software Threats Data Feed: сравнивать пакеты, полученные с помощью сервиса, с пакетами, используемыми в процессе разработки, по одному или нескольким параметрам (например, по имени пакета, по версии и т.д.).

Формат JSON выбран как наиболее оптимальный для парсинга и интеграции в различные решения, используемые в процессе разработки.



Точки интеграции

1

На этапе загрузки пакетов из репозиториев с открытым исходным кодом (точка интеграции — проксирующий репозиторий).

2

На этапе компиляции разработчиком исходного кода, в том числе с включением в сборку зависимых пакетов, которые могут представлять угрозу (точка интеграции — конвейер).

3

На этапе публикации исходного кода в репозиторий (точка интеграции — механизм публикации).

Рекомендация в случае обнаружения проблемного пакета — действовать в соответствии с политикой, принятой в организации (уведомление разработчика, обработка рисков, блокировка и т. д.).

Поток данных Kaspersky Open Source Software Threats Data Feed внесён в российский Реестр программного обеспечения.

Подробнее

Kaspersky Threat Intelligence

Подробнее

www.kaspersky.ru

#kaspersky
#активируйбудущее