SOLAR APPSCREENER

БЕЗОПАСНОСТЬ OPEN SOURCE ПОД КОНТРОЛЕМ

В популярном open-source-пакете node-ipc был обнаружен вредоносный код, который удалял файлы на компьютере пользователей с IP из России и Белоруссии.

Кейс node-ipc — это яркий пример атаки на цепочку поставки, то есть атаки, которая реализуется через сторонних поставщиков ПО. В рамках такой атаки злоумышленник не взламывает системы защиты компании, а идет другим путем — например, заражает open-source-библиотеки, которые могут использоваться для разработки ПО жертвы и под видом легитимного софта попадают в периметр компании.

В результате злоумышленник может воспользоваться уязвимостью в стороннем компоненте и получить доступ к инфраструктуре компании.

Такие атаки могут привести к серьезным последствиям — от юридических проблем и утечек конфиденциальных данных до больших денежных и репутационных потерь.

>630%

рост числа атак на цепочку поставок за последний год

45%

компаний по всему миру столкнутся supply-chain-атаками к 2025 году

ДАННЫЕ SONATYPE, GARTNER

КАК ЗАЩИТИТЬСЯ ОТ АТАК НА ЦЕПОЧКУ ПОСТАВОК ПО?

Лучший способ обезопасить свою цепочку поставок ПО — проверять безопасность всех сторонних библиотек и компонентов, которые вы используете в собственных разработках, и внедрить контроль защищенности кода на каждом этапе разработки. Это поможет вовремя выявить уязвимости в коде и устранить их, пока цена ошибки еще не так высока.

Проверить безопасность цепочки поставок ПО и open-source-компонентов помогут следующие технологии:

- Анализ состава ПО (Software Composition Analysis, SCA)
- Анализ supply chain (Supply Chain Security, SCS)

Эти технологии входят в состав Solar appScreener — инструмента для комплексного контроля безопасности ПО на всех этапах разработки.

КАК РАБОТАЕТ КОНТРОЛЬ OPEN SOURCE В SOLAR APPSCREENER

SOFTWARE COMPOSITION ANALYSIS (SCA)

- Анализирует состав разрабатываемого ПО.
- Находит в нем сторонние компоненты и выявляет в них уязвимости и закладки.
- Обнаруживает зависимости и связи с другими библиотеками внутри ПО.

SUPPLY CHAIN SECURITY (SCS)

- Контролирует безопасность open source на протяжении всего пути, по которому компоненты попадают в компанию, — от их создания или покупки обновлений до их использования в разработке.
- Отслеживает подозрительную активность в сторонних библиотеках и дает комплексную оценку их безопасности на основе 8 конкретных критериев:
  - Популярность библиотеки
  - Авторский состав
  - Реакция сообщества на проблемы с безопасностью компонента
  - Уровень заинтересованности авторов в безопасности компонента
  - Дата создания библиотеки
  - Является ли эта версия первым релизом компонента
  - Необходимое количество проектов у разработчика компонента
  - Количество code review, которые проводятся как минимум двумя рецензентами

ОЦЕНКА ЛИЦЕНЗИОННЫХ РИСКОВ

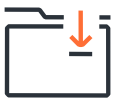
- Выявляет возможные риски, связанные с лицензированием open source: отсутствие лицензии, несовместимость лицензий нескольких компонентов, нарушение политик лицензирования и другие.
- Отвечает на вопрос, можно ли использовать конкретную библиотеку согласно ее лицензионной политике.

ЗАЧЕМ ВНЕДРЯТЬ SOLAR APPSCREENER ДЛЯ КОНТРОЛЯ БЕЗОПАСНОСТИ OPEN SOURCE

1. Полноценный контроль заимствованных компонентов в вашем ПО с помощью одного инструмента
2. Предотвращение supply-chain-атак и угроз, связанных с общедоступными библиотеками
3. Выявление уязвимостей и закладок в сторонних компонентах на ранних этапах разработки и экономия ресурсов на их исправление перед релизом
4. Меньше юридических рисков из-за отсутствия, несовместимости и других проблем с лицензиями сторонних компонентов
5. Управление рисками ИБ из-за использования заимствованного кода

ЧТО ВЫ ЗАГРУЖАЕТЕ НА АНАЛИЗ

Исходный код ПО



Ссылки на репозиторий

SBOM-файл

ЧТО ВЫ ПОЛУЧАЕТЕ В РЕЗУЛЬТАТЕ АНАЛИЗА

1. Перечень всех сторонних компонентов в коде приложения
2. Список всех уязвимостей и зависимостей в сторонних компонентах
3. Оценка безопасности используемых open-source-компонентов на основе 8 метрик
4. Рекомендации, как устранить потенциальные угрозы
5. Информация о юридических рисках, связанных с лицензионной политикой заимствованного ПО

ПРЕИМУЩЕСТВА SOLAR APPSCREENER

Комплекс передовых технологий, который полностью решает задачу управления безопасностью сторонних компонентов ПО

Эффективная защита от supply-chain-атак и других угроз, связанных с использованием библиотек с открытым исходным кодом

Оценка безопасности компонентов основана на четких метриках, учитывающих репутацию автора ПО, популярность компонента и другие параметры

Удобная интеграция решения в цикл безопасной разработки ПО (Secure SDLC)

ТЕСТИРОВАТЬ БЕСПЛАТНО

T +7 (499) 755-07-70
E info@rt-solar.ru

Центральный офис, 125009, Москва
Никитский переулок, 7с1

SOLAR