Ростелеком
Солар

Solar appScreener

Новые вызовы в области безопасной разработки: как обеспечить безопасность кода в современных реалиях

Станислав Лукьяненко

Директор по работе с заказчиками
компании "Ростелеком-Солар"

Ситуация сегодня

90% компаний

под защитой «Ростелеком-Солар» ежедневно подвергаются DDoS-атакам с использованием заграничных ботнетов

Массовые атаки на веб-ресурсы: дефейс через взлом счетчиков и баннеров (репутационный урон)

Повышение активности проправительственных группировок (проникновение в ОКИИ и госсектор)

Необратимое шифрование данных без возможности выкупа

Эксплуатация новых критических уязвимостей

Встраивание ВПО в Open Source

Ростелеком Солар

Чего стоит опасаться?

Уязвимости

Неумышленные ошибки, нестыковки, неточности, которые ведут к возможности взлома системы

Закладки (НДВ*)

Скрытая функциональность, умышленно внесенная в код, в т.ч. СПО, библиотеки

* Недекларированные возможности

Ростелеком Солар

НДВ в open-source компонентах

CVE-2022-23812 зарегистрирован в марте 2022 г.

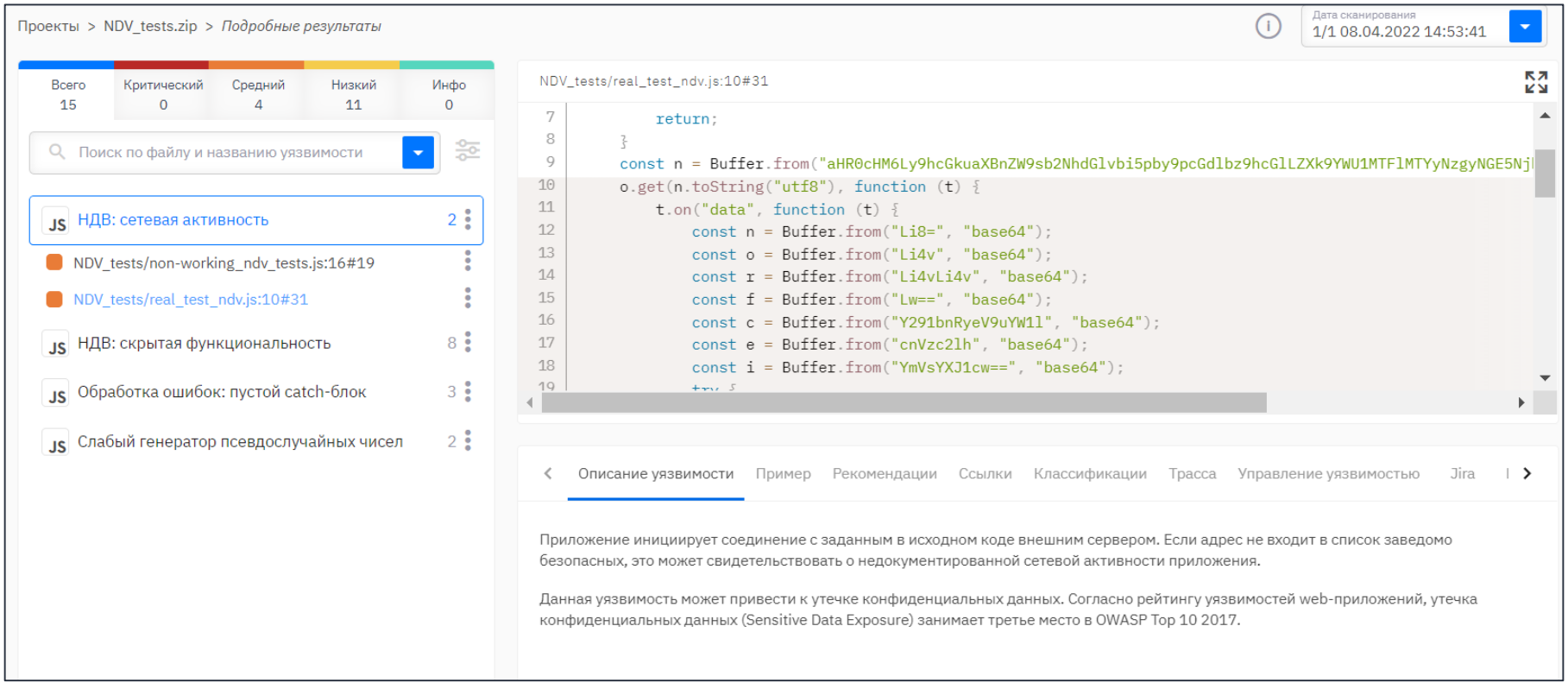
Пакет **node-ipc** версий от 10.1.1 до 10.1.3 содержит вредоносный код

node-ipc загружают более 1 млн раз в неделю

Рекомендация: при использовании open-source компонентов необходима обязательная проверка на наличие уязвимостей и НДВ средствами **SAST** и **SCA**

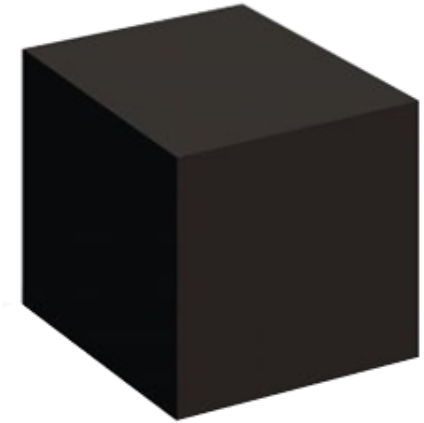
Ростелеком Солар

Solar appScreener – НДВ: скрытая функциональность



Ростелеком Солар

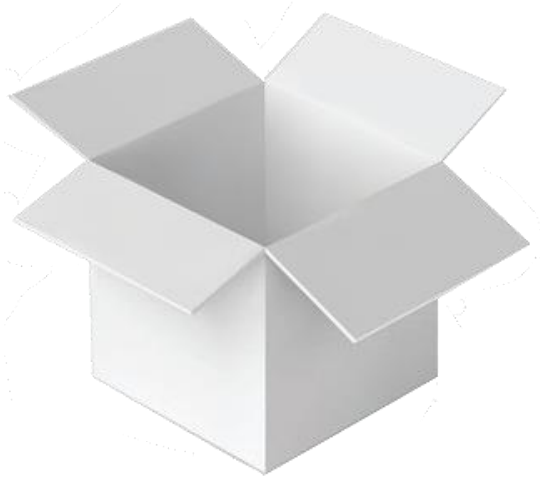
Решение – Solar appScreener



Исполняемые файлы
(бинарный код)

appScreener

Уникальные технологии
декомпиляции и деобфускации



Исходный код
для SAST

Ростелеком
Солар

Анализ исходного кода – 36 языков

Ростелеком Солар

Анализ бинарного кода – 9 форматов файлов

Для мобильных приложений достаточно скопировать ссылку из Google Play или App Store

Приложение будет автоматически:

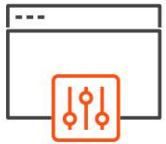
1 Скачано → 2 Декомпилировано и деобфусцировано → 3 Проверено

Ростелеком Солар

Основные преимущества

Умеет работать без исходных кодов

Не надо просить исходные коды у разработчиков – можно получить файлы для анализа у системного администратора или дать ссылку на Google Play или App Store



Не требует опыта разработки

Solar appScreener рассчитан на службу ИБ, а не на разработчиков.
Для работы с ним не нужно знать программирование и проходить специальное обучение

Дает понятные рекомендации

Офицеру безопасности предоставляются подробные описания найденных уязвимостей
и НДВ, а также рекомендации по настройке WAF*

*Web Application Firewall – межсетевой экран уровня приложений (L7 модели OSI)

Ростелеком Солар

Основные преимущества

Минимизирует ложные срабатывания

Уникальная технология Fuzzy Logic Engine позволяет минимизировать процент ложноположительных и ложноотрицательных срабатываний

Отчеты могут формироваться в соответствии с классификацией уязвимостей по версии PCI DSS, БДУ ФСТЭК России, ОУД4, OWASP Top 10 и Mobile Top 10, HIPAA и CWE/SANS Top 25

Легко интегрируется в SDLC*

Реализована интеграция с репозиториями Git и Subversion, VCS хостингами GitLab, GitHub, Bitbucket, средствами разработки Eclipse, Visual Studio и IntelliJ IDEA, средствами сборки Xcode, CMake, Visual Studio, GNU Make, GNU Autotools, Gradle, sbt, Maven, серверами CI/CD Jenkins, Azure DevOps Server и TeamCity, платформой анализа качества кода SonarQube, а также системой отслеживания ошибок Atlassian Jira

*Software Development Life Cycle – жизненный цикл разработки ПО

Ростелеком Солар

Возможности интеграции

Репозитории

VCS хостинги

Средства разработки

Средства сборки

Серверы CI/CD

Отслеживание задач

Анализ кода

Открытый API предоставляет широкие возможности по дополнительной интеграции и автоматизации. Включает в себя JSON API и CLI.

Ростелеком
Солар

Требования регуляторов

Внесен в Единый реестр отечественного ПО (№ 7763)
и сертифицирован ФСТЭК России на соответствие требованиям
по 4-му уровню доверия (сертификат № 4007) и ТУ

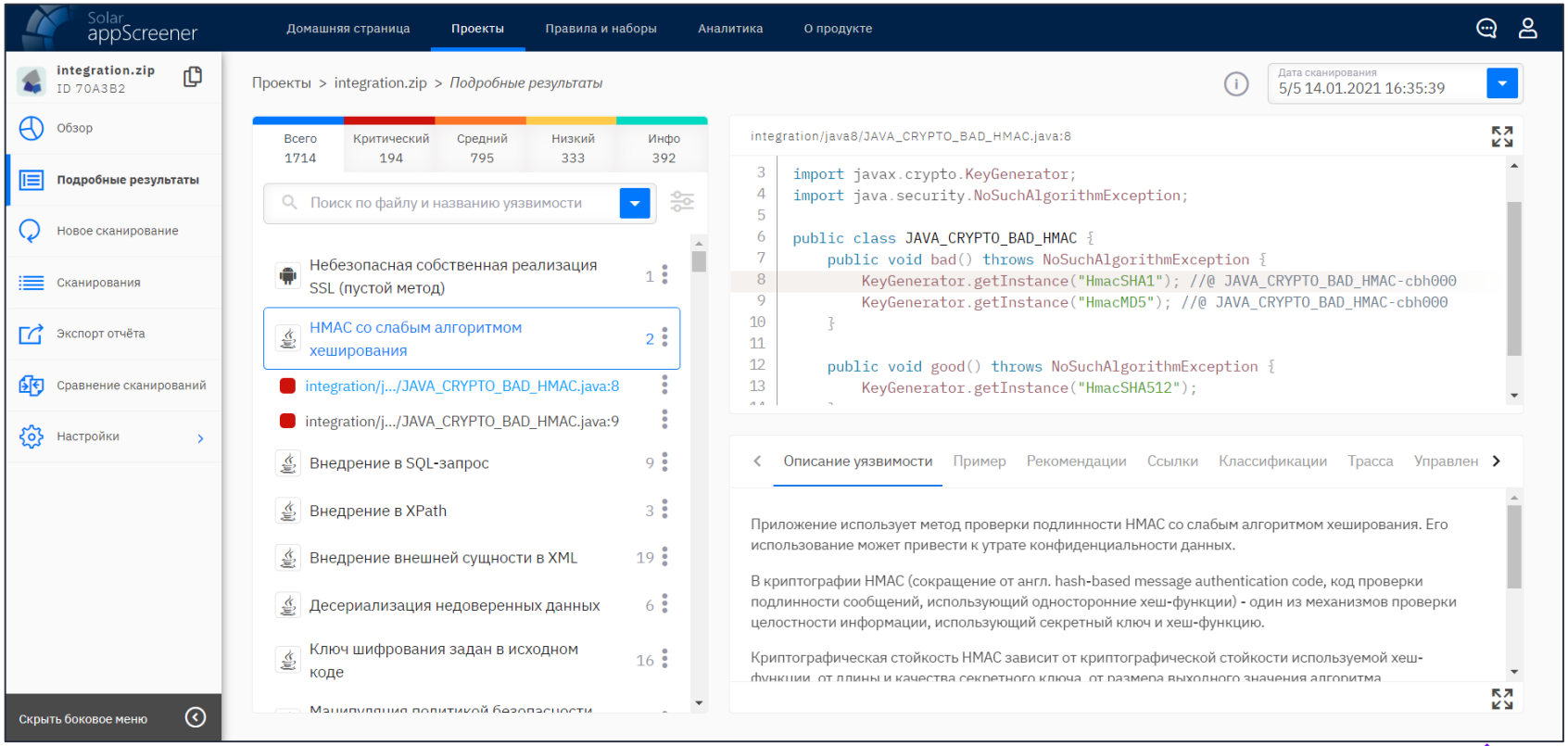
Банк России

Помогает выполнять постановления 683-П, 719-П, 757-П Банка России в части
анализа защищенности ПО и оценке соответствия по требованиям ОУД 4

Соответствует приказам 239, 76, и требованиям ГОСТ Р 56939-2016
ФСТЭК России в части анализа защищенности и исходного кода ПО

Ростелеком
Солар

Графический интерфейс



Ростелеком Солар

Публичные клиенты

МТС Банк

S7 AIRLINES

МСП Банк

CARTREK
innovative cars sharing platform

ВСЕРОССИЙСКИЙ БАНК РАЗВИТИЯ РЕГИОНОВ

Яндекс Деньги

ISBC
RFID

MSOFT

ББР БАНК

nexagate

Sense of Security

Ак Барс Банк

ATABASCA

PARASOFT

KISA
Korea Internet & Security Agency

РЖД Федеральная Пассажирская Компания

Compliance Control

EXANTE

ВТБ МОБАЙЛ

ЛИГА СТАВОК

ДОМОДЕДОВО
МОСКОВСКИЙ АЭРОПОРТ

БАНК ЗЕНИТ

Ростелеком Солар

Лицензирование и поставка

Установка на собственный сервер (On-premise)

- Лицензирование осуществляется по количеству пользователей, которые имеют доступ к системе
- Подходит при необходимости постоянного анализа ПО (крупные вендоры и компании)

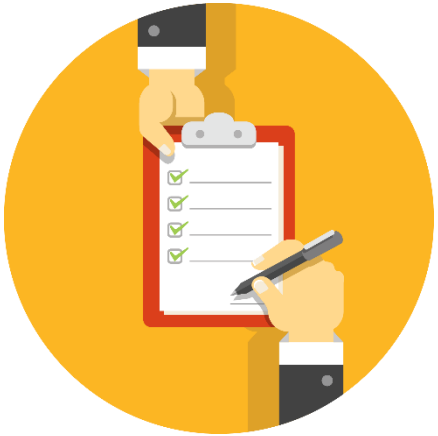
Сервис из облака «Ростелеком-Солар» (SaaS)

- Оплачивается количество произведенных проверок
- Подходит, если потребность в проверке приложений возникает время от времени (небольшие вендоры, использование заказного ПО, «перестраховка»)

Ростелеком Солар

План действий

1. Получить доступ к демостенду Solar appScreener, написав на s.lukyanenko@rt-solar.ru
2. Совместно оценить потребности организации в анализе кода
3. Инициировать пилотный проект
4. Успешно реализовать пилот



Ростелеком
Солар