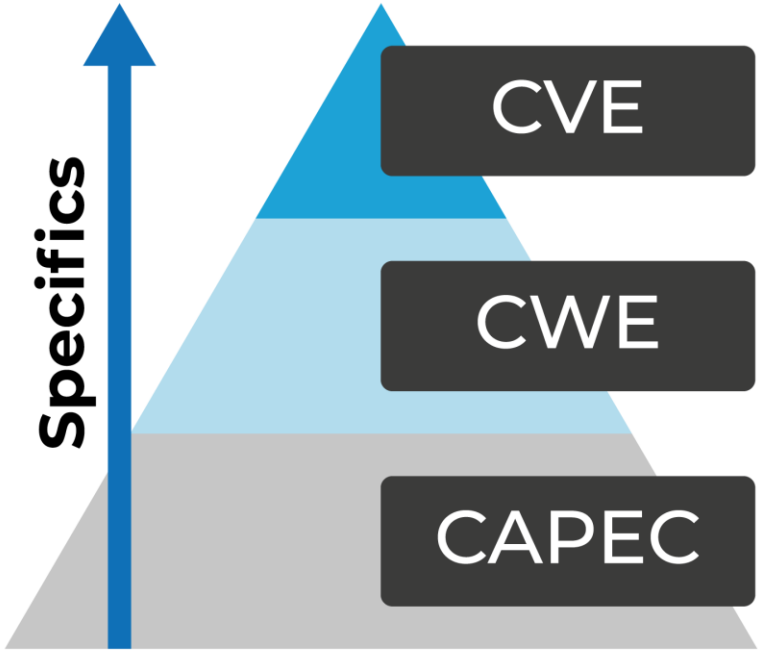
КОД безопасности

Развитие системы выявления и устранения уязвимостей на примере внедренных процессов в ООО «Код Безопасности»

Дмитрий Подшибякин (начальник отдела безопасной разработки)

КОД безопасности

Классификация уязвимостей



Common Vulnerability Enumeration

- Vendor specific
- Identified, validated vulnerabilities

Common Weakness Enumeration

- Vendor agnostic
- Categories of exploitable errors based on historical vulnerabilities

Common Attack Pattern Enumeration and Classification

- Implementation agnostic
- Threat modeling
- Vulnerability and exploit identification approach

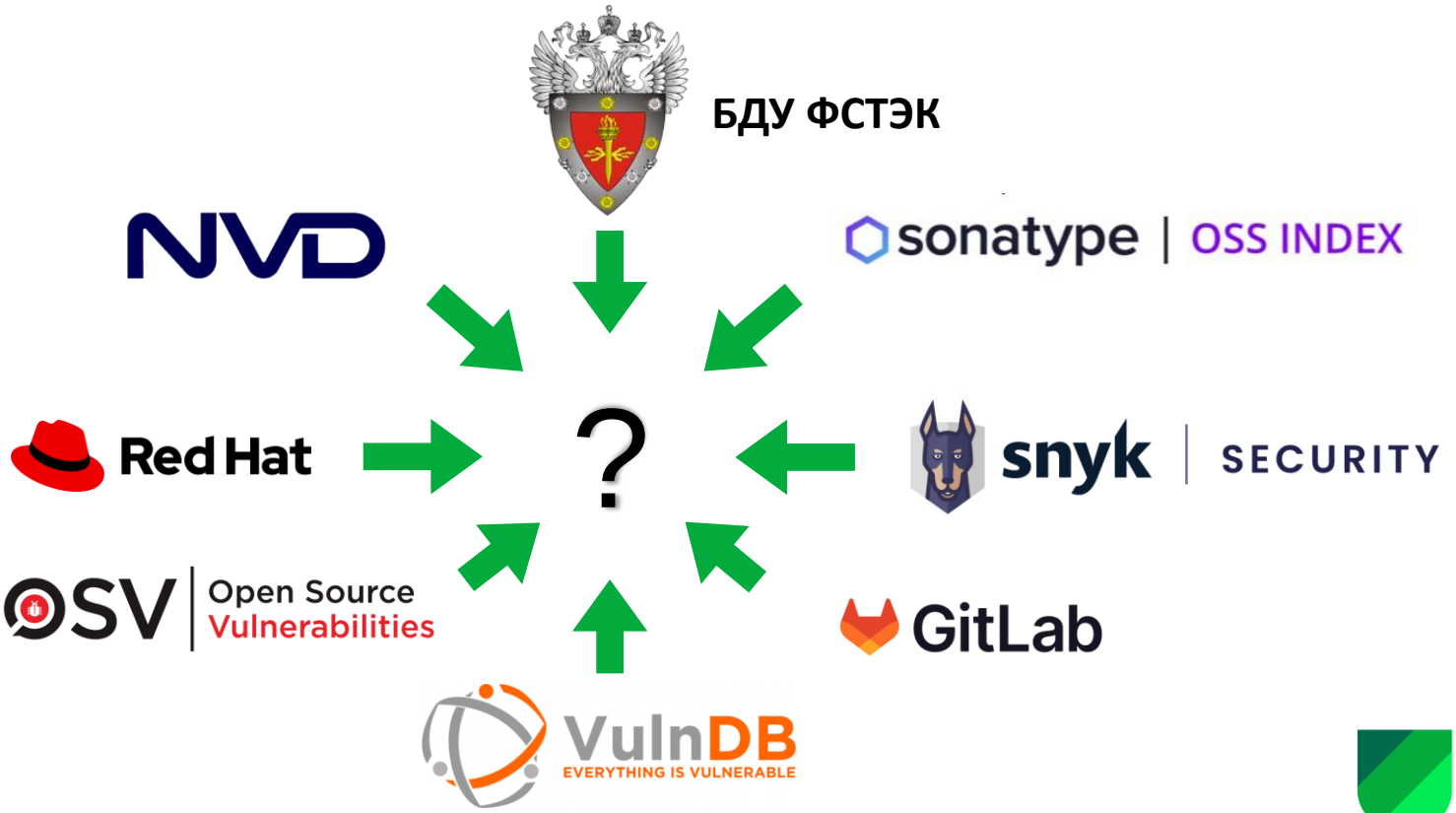
КОД безопасности

CVE (Common Vulnerabilities and Exposures)

CVE (Common Vulnerabilities and Exposures) — общеизвестные уязвимости информационной безопасности.

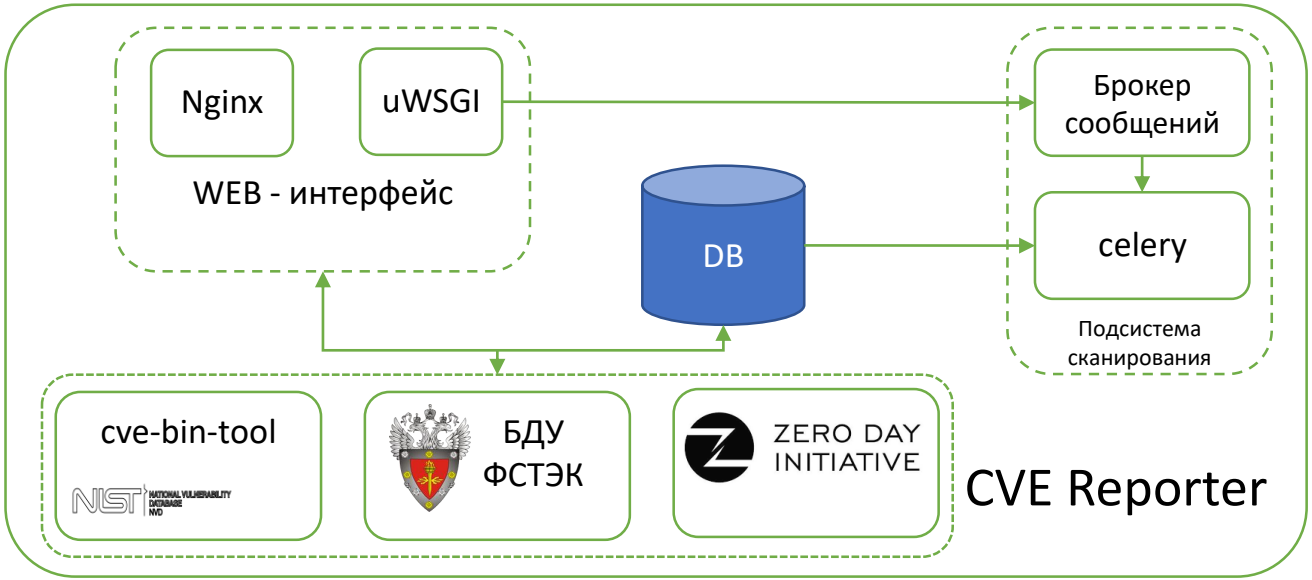
КОД безопасности

Базы данных CVE



КОД безопасности

Архитектура CVE Reporter



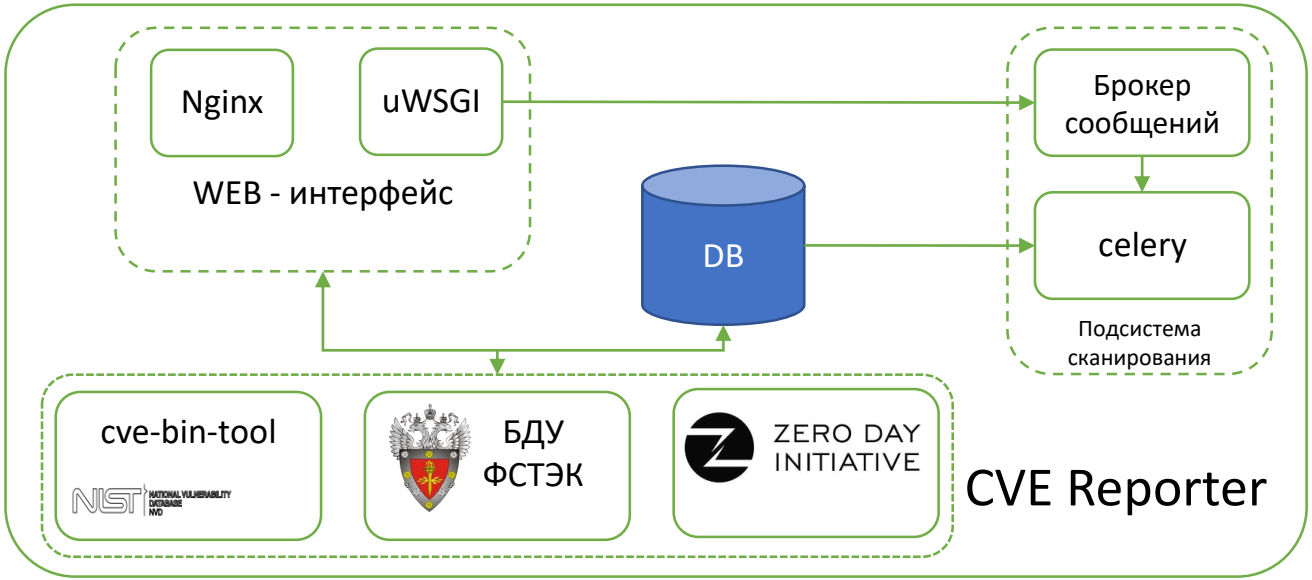
КОД безопасности

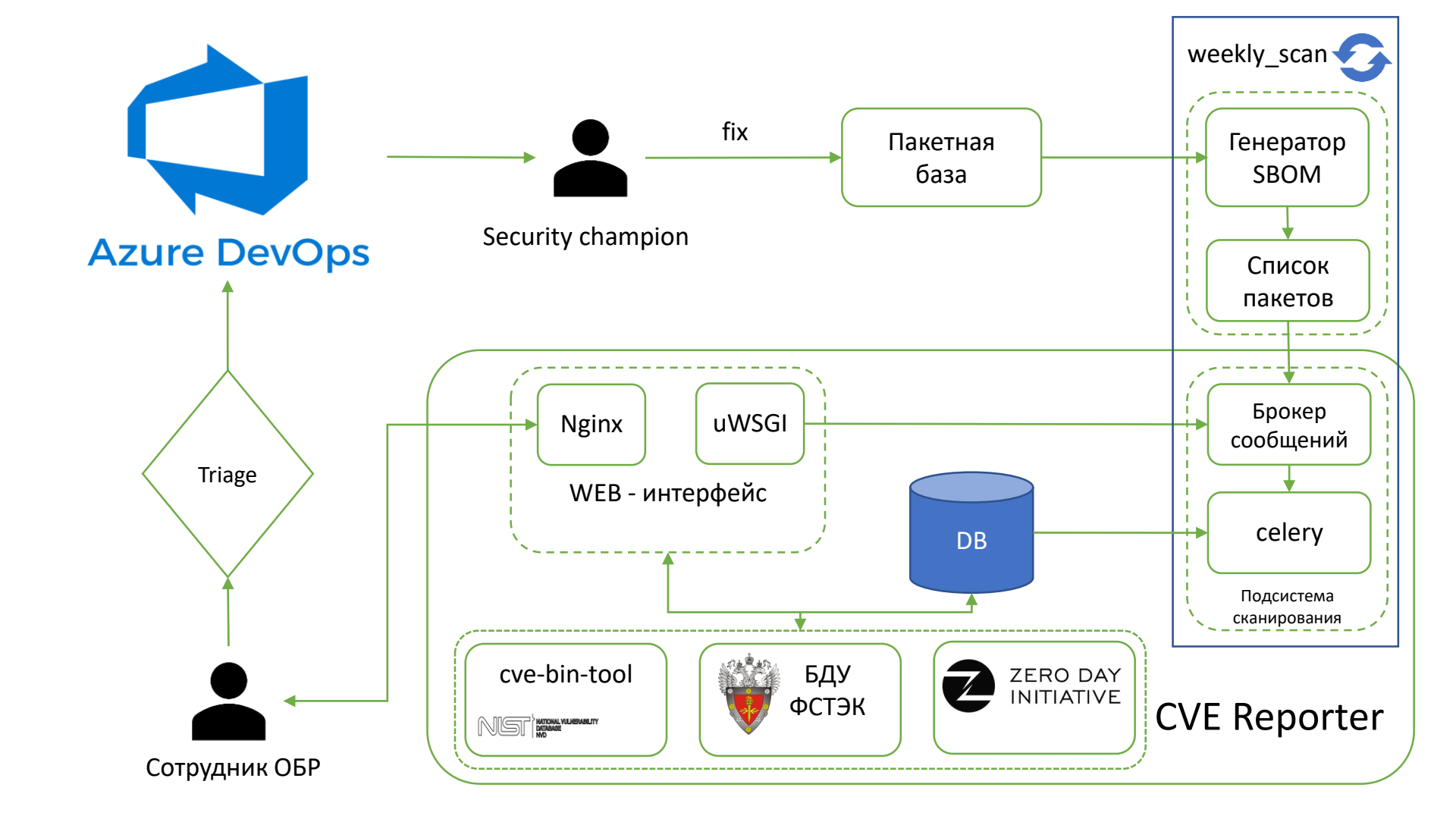
Архитектура CVE Reporter

Основу CVE Reporter составляет консольная утилита cve-bin-tool, которая загружает информацию из различных источников, в частности: NIST, Red Hat, OSV, GitLab. К этим источникам была добавлена БДУ ФСТЭК.

В процессе развития CVE Reporter был добавлен ZDI.

Регулярно проводится оценка необходимости и возможности добавления других источников.



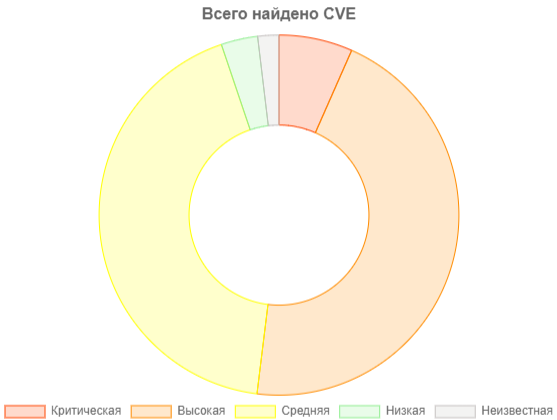

Azure DevOps
Security champion
fix
Пакетная база
weekly_scan
Генератор SBOM
Список пакетов
Брокер сообщений
celery
Подсистема сканирования
Nginx
uWSGI
WEB - интерфейс
DB
Triage
cve-bin-tool
NIST NATIONAL VULNERABILITY DATABASE NVD
БДУ ФСТЭК
ZERO DAY INITIATIVE
CVE Reporter
Сотрудник ОБР

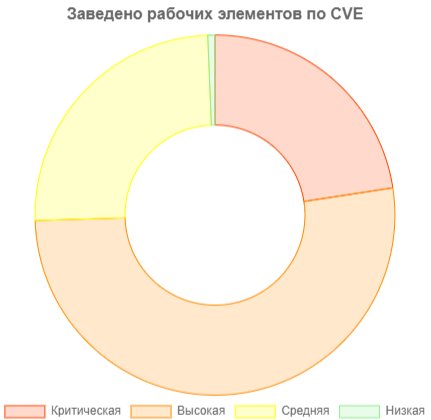
Продуктов: 45

Всего CVE: 24991

Необработанных CVE: 2756

Заведено рабочих элементов: 320





JinnServer

Система массовой проверки и формирования электронной подписи в юридически значимом электронном документообороте

SNLSP

Средство защиты информации от несанкционированного доступа для операционных систем семейства Linux

SNS

Защита данных и инфраструктуры серверов и рабочих станций

vGate

Средство микросегментации и защиты жизненного цикла виртуальных машин

ZTN

Клиентское приложение для защищенного доступа в корпоративную сеть с удаленных персональных компьютеров и смартфонов сотрудников

Континент-3

Централизованный комплекс для защиты сетевой инфраструктуры и создания VPN-сетей с использованием алгоритмов ГОСТ

Континент-4

Многофункциональный межсетевой экран (NGFW/UTM) с поддержкой алгоритмов ГОСТ

Континент-TLS

Система обеспечения защищенного удаленного доступа к веб-приложениям с использованием алгоритмов шифрования ГОСТ

Соболь

Надежный программно-аппаратный комплекс обеспечивает доверенную загрузку операционной системы

Скопировать | CSV | Excel | PDF | Print

Фильтр:

Отображены строки с 1 по 2,158 (всего 2,158)

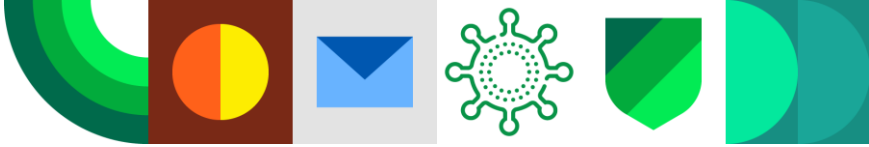
Продукт	CVE	Критичность	Пакет	Версия	Обоснование	Статус
Тестовый продукт	CVE-2023-27536	Средняя	curl	7.61.1		NewFound
Тестовый продукт	CVE-2023-32001	Средняя	curl	8.0		NewFound
Тестовый продукт	CVE-2018-16839	Критическая	curl	7.61.1		NewFound
Тестовый продукт	CVE-2018-16840	Критическая	curl	7.61.1		NewFound
Тестовый продукт	CVE-2021-22926	Высокая	curl	7.61.1		NewFound
Тестовый продукт	CVE-2022-43552	Средняя	curl	7.61.1		NewFound
Тестовый продукт	CVE-2023-23916	Средняя	curl	7.61.1		NewFound
Тестовый продукт	CVE-2023-28319	Высокая	curl	8.0		NewFound
Тестовый продукт	CVE-2023-28322	Низкая	curl	7.61.1		NewFound
Тестовый продукт	CVE-2022-32221	Критическая	curl	7.61.1		NewFound

КОД безопасности

Планы по дальнейшему развитию

- Добавление других методов анализа
- Увеличение количества используемых источников
- Собственная метрика оценивания
- Автоматическое создание задач на исправление (данный функционал уже реализован, но еще не внедрен)

КОД безопасности



Спасибо за внимание!

info@securitycode.ru
www.securitycode.ru