

Система анализа и мониторинга состояния ИБ DATARK

Тема 5. Настройка проверок на уязвимости и
соответствие требованиям информационной
безопасности.

Общие сведения

Уязвимости:

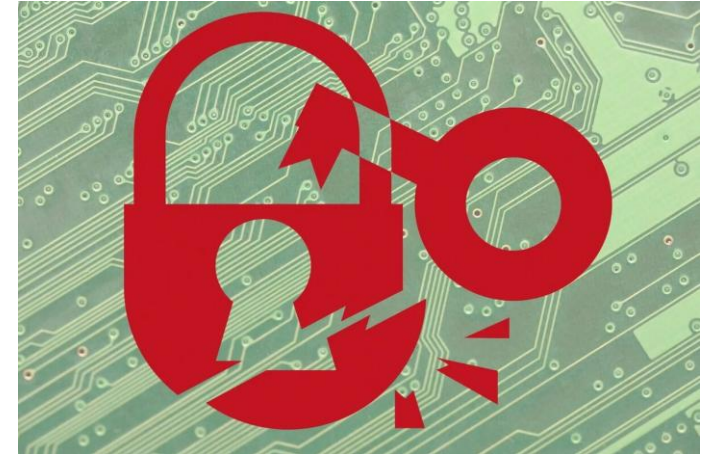
1. ошибки в коде, снижающие уровень безопасности в системе
2. ошибки в настройках / недостаточно безопасная конфигурация (снижают безопасность сильнее, чем (1))

Режимы сканирования:

- аудит (подключение к активу, сбор необходимых данных, интерпретация) – используется в DATAPK
- pentest – попытка в некотором виде проэксплуатировать уязвимость – часто запрещено в АСУ ТП, отсутствует в DATAPK

Обычно (1) устраняется обновлением ПО, что в технологических сетях зачастую затруднительно и не всегда возможно в принципе (работа техпроцесса приоритетнее / надо тестировать обновления, не всегда АСУ ТП на вендорской поддержке / совместимы с современными ОС и пр.)

А вот (2) – это необходимая гигиена, которая позволит существующими средствами сильно снизить поверхность атаки (это не отменяет тестирования на совместимость, но в реализации обычно проще)



Поиск уязвимостей в DATAPK

Модуль Configuration Management (CM)

- сбор конфигураций + проверка на соответствие заданным настройкам (можно корректировать под внутренние регламенты);
- сканеры с типом «Версия ОС» и «Установленное ПО» - их результаты используются для поиска уязвимостей;
- сканеры сбора для сбора OVAL-объектов

Модуль Vulnerability Management (VM)

- **OVAL** – открытый стандарт описания состояния активов, есть базы CIS, БДУ ФСТЭК России, но инструмент сбора информации с активов имеет существенные ограничения (обязательно опрашивать актив здесь и сейчас, много запросов в сторону актива, не поддерживаются ПЛК и пр.), в ближайшее время планируется к исключению из DATAPK (в курсе не рассматривается). Базы поставляются производителем DATAPK.
- **CVE2CPE** – альтернативный механизм – с помощью сканеров сбора типа «Версия ОС» и «Установленное ПО» собирается информация с активов, преобразуется в CPE (поля Vendor, Product, Version), и осуществляется поиск уязвимостей для этих ОС/прошивок/ПО по базе CVE и БДУ ФСТЭК России. Поиск можно проводить без обращения к активу «здесь и сейчас» (по ранее собранному слепку, например в режиме ТО). Производитель DATAPK предоставляет обновления баз, таблицы маппинга (как интерпретировать собранные данные с актива в формат CPE).

Проверка настроек безопасности

Конфигурация WinCC7 (noport) (SQL)		Просмотр	Сравнение
Настройки проекта Siemens WinCC (winrm https-basic)			
Общие файловые ресурсы (winrm https-basic)			
Параметры сетевых интерфейсов (winrm https-basic)			
Приказ ФСТЭК 239 (winrm https-basic)			
Проверка настроек безопасности Windows			
Список пользователей и их группы (winrm https-basic)			

№	Настройка	Статус	Должно быть	Имеется
2	Максимальный срок действия пароля (в днях)	Соответствует	-1	-1
3	Минимальная длина пароля (количество симво...	Не соответствует	12	8
4	Пароль должен отвечать требованиям сложности	Не соответствует	1	0
5	Вести журнал паролей	Соответствует	12	12
6	Пороговое значение блокировки (попытки)	Не соответствует	5	0
7	Время до сброса счетчика блокировки (в минут...	Не соответствует	10	
8	Продолжительность блокировки учетной запис...	Не соответствует	10	
9	Хранить пароли, используя обратимое шифров...	Соответствует	0	
10	Доступ к этому компьютеру из сети	Не соответствует	Administrators	
11	Архивация файлов и каталогов	Не соответствует	Administrators	

- рекомендации вендоров ОС/ПО
- рекомендации регуляторов
- рекомендации вендоров СЗИ / интеграторов
- стандарты организации

Конфигурация WinCC7 (noport) (SQL)		Просмотр	Сравнение
Настройки проекта Siemens WinCC (winrm https-basic)			
Общие файловые ресурсы (winrm https-basic)			
Параметры сетевых интерфейсов (winrm https-basic)			
Приказ ФСТЭК 239 (winrm https-basic)			
Проверка настроек безопасности Windows			
Список пользователей и их группы (winrm https-basic)			

№	Правило	Статус	Должно быть	Имеется
10	4.4 Ограничение прав группы пользователей SIMATIC...	Ознакомление	Отсутствие учетных записей	Настройка отсут...
11	4.5 Настройка БД MSSQL для работы системы монит...	Соответствует	1433	1433
12	5.3 Отключение приложений диагностики, которые м...	Соответствует	Отсутствие процессов: WinCCDia...	-
13	Проверка сетевых интерфейсов на отключение IPv6	Не соответствует	Отключено	Loopback Pseudo...
14	6.1 Запуск WinCC Runtime в качестве системной служ...	Ознакомление	Service	Неизвестный
15	6.2 Отключение стандартных сочетаний клавиш Wind...	Не соответствует	Отключено	ctrl+esc
16	6.3 Изменение свойств проекта	Ошибка	list index out of range	Параметр не мо...
17	7.2 Пароль администратора в User Administrator	Соответствует	Отсутствие пользователей с паро...	

CIS Network Parameters (Host Only) (ssh)		Просмотр	Сравнение
xml-configuration-scadabr			
Список пользователей Unix (ssh)			
Список устройств Unix (ssh)			
Таблица маршрутизации Unix (ssh)			
ФСТЭК России рекомендации по обеспечению безопасной настройки ОС Linux			

№	Проверка	Пункт	Результат	Текущее значение	Эталонное зна
1	Настройка авторизации в операционной системе	Запрет учётных записей пользоват...	Соответствует	/etc/pam.d/password-...	/etc/pam.d/pass...
2	Настройка авторизации в операционной системе	Отключение входа суперпользоват...	Не соответствует	PermitRootLogin yes	PermitRootLogin
3	Настройка механизмов защиты ядра Linux	Блокировка утечки информации об...	Не соответствует	kernel.kptr_restrict = 1	kernel.kptr_restr
4	Настройка механизмов защиты ядра Linux	Включена защита подсистемы eBPF	Не соответствует	net.core.bpf_jit_harde...	net.core.bpf_jit_
5	Настройка механизмов защиты ядра Linux	Запрет слияния кэшей slab-аллока...	Не соответствует	Не найдено	slab_nomerge =
6	Настройка механизмов защиты ядра Linux	Инициализация механизма IOMMU	Не соответствует	Не найдено	iommu = force
7	Настройка механизмов защиты ядра Linux	Инициализация механизма IOMMU	Не соответствует	Не найдено	iommu.strict = 1

Как реагировать на отклонения:

- *устранять в первую очередь / запланировать устранения в ТО (после тестов на невлиание)*
- *в случае ошибок сбора – скорректировать сканер (воспользоваться рекомендациями из темы 3)*

Поиск уязвимостей (CVE2CPE)

Сперва нужно собрать информацию об ОС (прошивке) и перечень ПО (для АРМ/серверов – для ПЛК/АСО неприменимо)

Информация об ОС 

Изменен: 11.08.2025, 13:02:34

Производитель: ubuntu

Наименование: Ubuntu

Версия: 20.04.3 LTS (Focal Fossa)

Перечень ПО 1762 / 3799



Управление

Выберите представление 



Представление

Производитель ПО	Наименование ПО	Версия ПО	Наименование актива	Дата сбора
Ubuntu Developers <ubunt...	zlib1g-dev	1:1.2.11.dfsg-2ubuntu1.3	SCADABR	11.08.2025, 13:02:56
Ubuntu Developers <ubunt...	zlib1g	1:1.2.11.dfsg-2ubuntu1.3	SCADABR	11.08.2025, 13:02:56
Ubuntu Developers <ubunt...	zip	3.0-11build1	SCADABR	11.08.2025, 13:02:56

☐ Наименование сканера	Описание	Тип
☐		
☐ Версия ОС Windows (winrm http)	Сканер для сбора версии О...	Версия ОС
☐ Версия ОС Windows (winrm http-basic)	Сканер для сбора версии О...	Версия ОС
☐ Версия ОС Windows (winrm https)	Сканер для сбора версии О...	Версия ОС
☐ Версия ОС Windows (winrm https-basic)	Сканер для сбора версии О...	Версия ОС
☐ Версия ОС Windows (wmi)	Сканер для сбора версии О...	Версия ОС
☐ Версия ПЛК Allen Bradley	Сканер для сбора версии П...	Версия ОС
☐ Версия ПЛК Regul	Сканер для сбора версии П...	Версия ОС

☐ Наименование сканера	Описание	Тип
☐		
☐ Установленное ПО CentOS (os soft) (ssh)	Сканер для сбора установле...	Установленное ПО
☐ Установленное ПО Debian (os soft) (ssh)	Сканер для сбора установле...	Установленное ПО
☐ Установленное ПО Windows (winexe 0.8)	Сканер для сбора установле...	Установленное ПО
☐ Установленное ПО Windows (winexe 1.0)	Сканер для сбора установле...	Установленное ПО
☐ Установленное ПО Windows (winrm http)	Сканер для сбора установле...	Установленное ПО

Поиск уязвимостей (CVE2CPE)

Далее – выполнить поиск уязвимостей (предварительно д.б. импортированы справочники)

Обнаружение уязвимостей (CVE)

Справочники ПО и уязвимостей
(CPE и CVE) 

Сопоставление собранного сканерами
ПО со справочником CPE 

Справочник БДУ ФСТЭК России 

Инциденты



Ничего не
найдено

Уязвимости

7299 8987

46213

139655

77156

Просмотр уязвимостей: SCADABR

CVE	Оценка уязвимости	CVSS	БДУ ФСТЭК
CVE-2023-1523	Критический	10	
CVE-2020-13753	Критический	10	
CVE-2021-3781	Критический	9.9	BDU:2024-05832
CVE-2025-5914	Критический	9.8	
CVE-2025-1020	Критический	9.8	BDU:2025-02308
CVE-2025-1017	Критический	9.8	

Уязвимость CVE-2021-3781

Описание Рекомендации

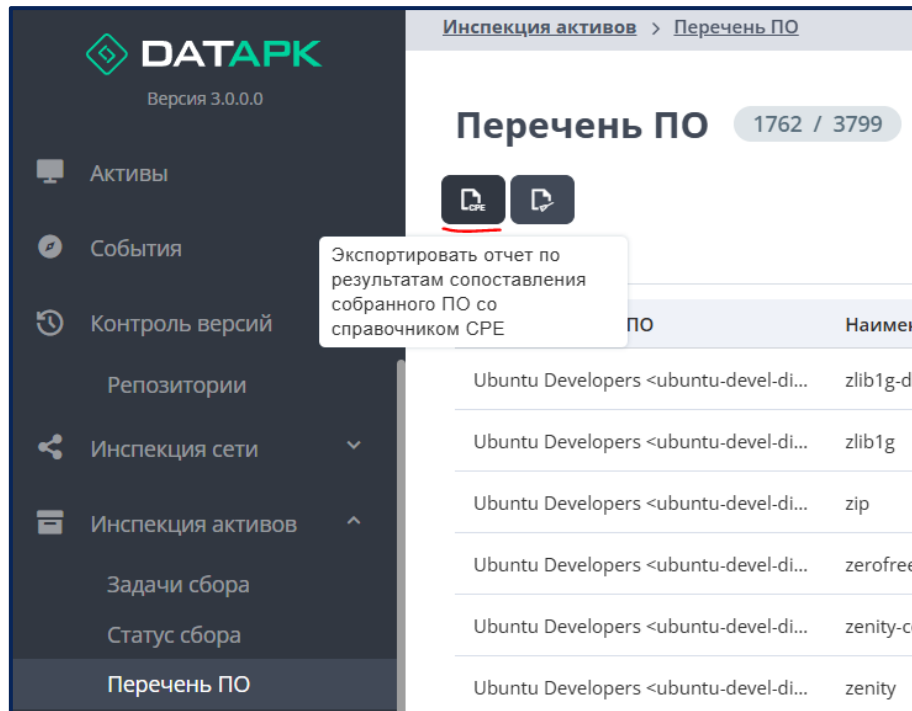
БДУ ФСТЭК России

BDU:2024-05832

Уязвимость набора программного обеспечения для обработки, преобразования и генерации документов Ghostscript связана с внедрением специально созданной команды `pipe`. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код

Поиск уязвимостей (CVE2CPE)

Для дополнения таблицы маппинга необходимо экспортировать отчет результатов сопоставления со страницы «Перечень ПО» и передать производителю DATAPK (после того, как выполнили сбор ОС и ПО со всего интересующего оборудования и выполнили поиск уязвимостей)



Соседняя кнопка «Очистить отчет по результатам сопоставления» обнуляет прошлый отчет, и после ее нажатия необходимо повторить поиск уязвимостей на узлах, с которых требуется передать информацию производителю DATAPK (крайне редкий кейс – в типовых инсталляциях ее нажимать не нужно).

Вопросы?