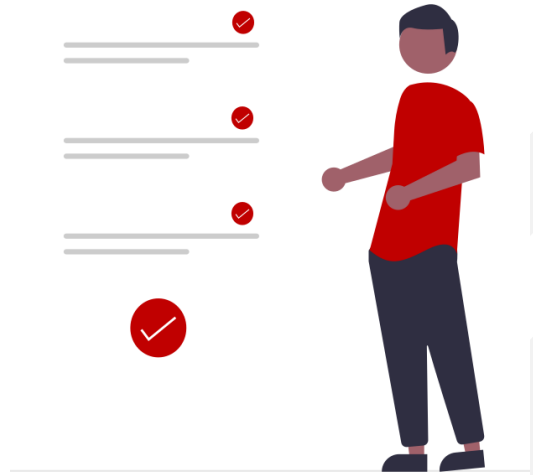
Эшелон
комплексная безопасность

Управление уязвимостями: процессы и инструменты

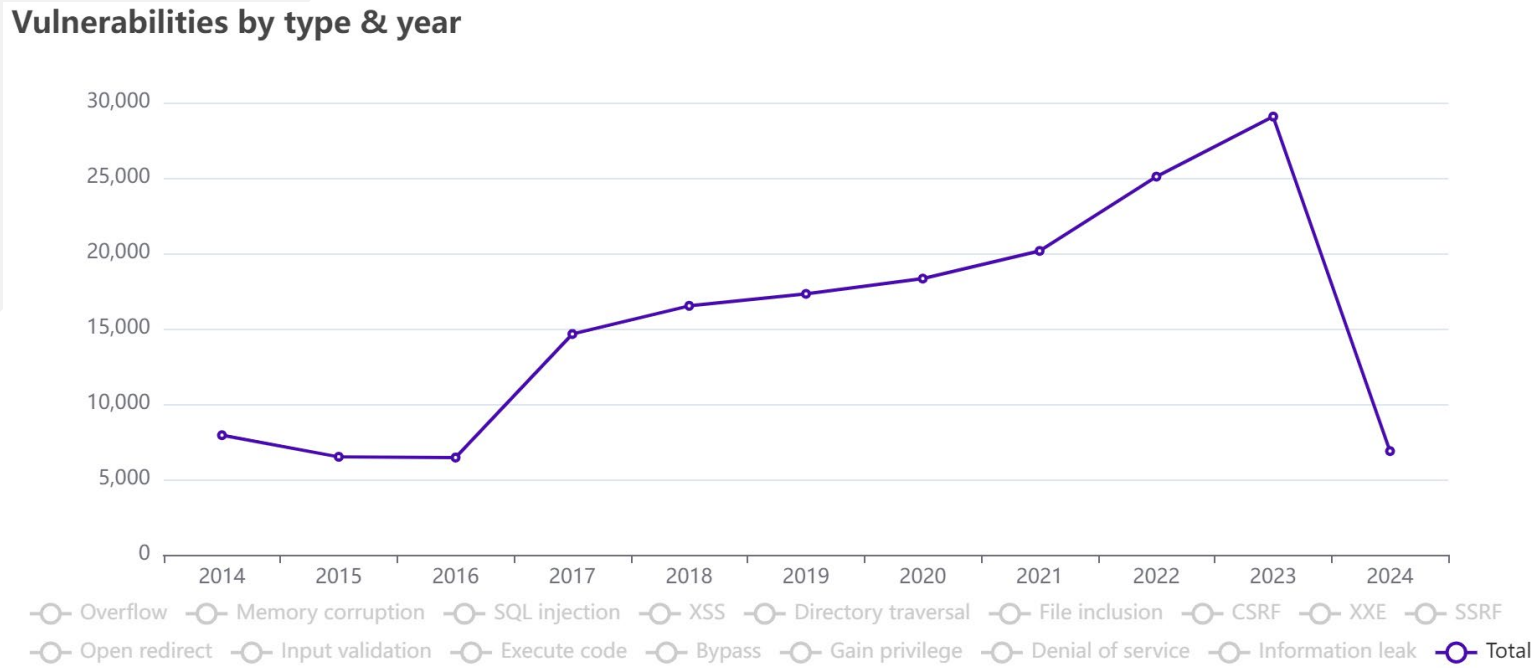
Александр Дорофеев | Генеральный директор АО «ЭШЕЛОН ТЕХНОЛОГИИ»

План

1. Актуальность борьбы с уязвимостями
2. Цикл управления уязвимостями
3. Выводы



Количество уязвимостей



В среднем публикуется более

70

уязвимостей в день

Источник: https://www.cvedetails.com/

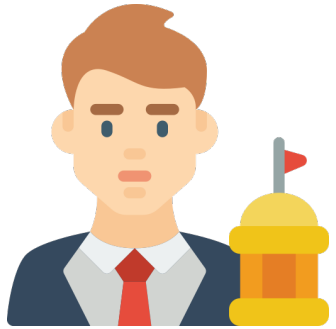
Какой процент реально опасных уязвимостей?

Источник: https://blog.qualys.com/vulnerabilities-threat-research/2023/12/19/2023-threat-landscape-year-in-review-part-one

Борьба с уязвимостями

- Разработчик:
  - Процессы разработки безопасного ПО

- Пользователь:
  - Процессы управления уязвимостями



- Регуляторы:
  - Требования к разработчикам СЗИ
  - Методические документы по управлению уязвимостями
  - Ведение базы данных угроз
  - Информирование об уязвимостях

Актуальность

ИСПДН

VIII. Контроль (анализ) защищенности персональных данных (АН3)					
АН3.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей		+	+	+
АН3.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	+	+	+	+
АН3.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации		+	+	+
АН3.4	Контроль состава технических средств, программного обеспечения и средств защиты информации		+	+	+
АН3.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе			+	+

ГИС

VIII. Контроль (анализ) защищенности информации (АН3)				
АН3.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей	+	+	+

АН3.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	+	+	+
АН3.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации	+	+	+
АН3.4	Контроль состава технических средств, программного обеспечения и средств защиты информации	+	+	+
АН3.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе	+	+	+

КИИ

XIV. Управление обновлениями программного обеспечения (ОПО)				
ОПО.0	Регламентация правил и процедур управления обновлениями программного обеспечения	+	+	+
ОПО.1	Поиск, получение обновлений программного обеспечения от доверенного источника	+	+	+
ОПО.2	Контроль целостности обновлений программного обеспечения	+	+	+
ОПО.3	Тестирование обновлений программного обеспечения	+	+	+
ОПО.4	Установка обновлений программного обеспечения	+	+	+

28. В рамках функционирования системы безопасности субъектом критической информационной инфраструктуры должны быть внедрены следующие процессы:

планирование и разработка мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры;

реализация (внедрение) мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры;

контроль состояния безопасности значимых объектов критической информационной инфраструктуры;

совершенствование безопасности значимых объектов критической информационной инфраструктуры.

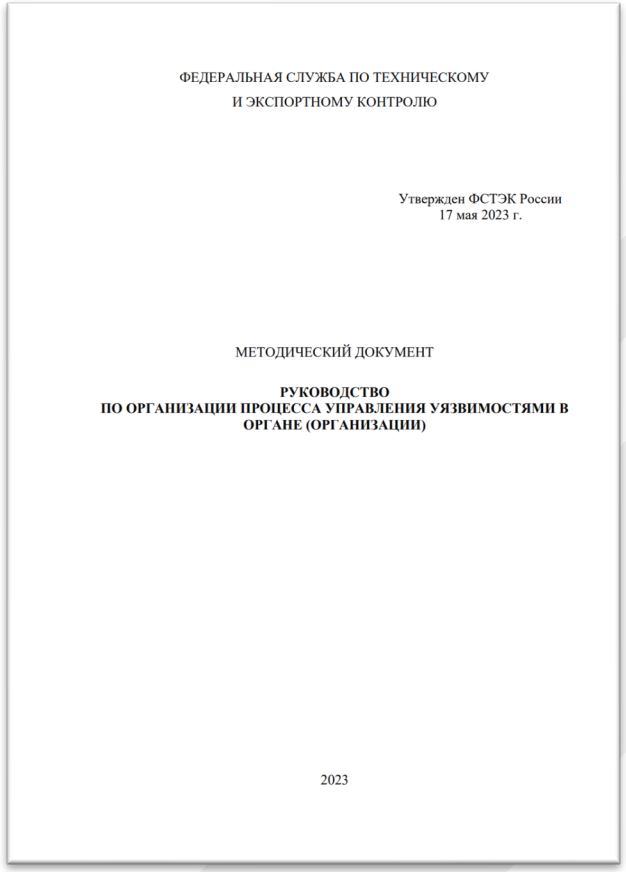
АСУ ТП

V. Аудит безопасности (АУД)				
АУД.0	Разработка политики аудита безопасности	+	+	+
АУД.1	Инвентаризация информационных ресурсов	+	+	+
АУД.2	Анализ уязвимостей и их устранение	+	+	+
АУД.3	Генерирование временных меток и (или) синхронизация системного времени	+	+	+
АУД.4	Регистрация событий безопасности	+	+	+
АУД.5	Контроль и анализ сетевого трафика			+
АУД.6	Защита информации о событиях безопасности	+	+	+
АУД.7	Мониторинг безопасности	+	+	+
АУД.8	Реагирование на сбои при регистрации событий безопасности	+	+	+
АУД.9	Анализ действий пользователей			+
АУД.10	Проведение внутренних аудитов	+	+	+
АУД.11	Проведение внешних аудитов			+

Руководство от ФСТЭК России

МЕТОДИЧЕСКИЙ ДОКУМЕНТ РУКОВОДСТВО ПО ОРГАНИЗАЦИИ ПРОЦЕССА УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ В ОРГАНЕ (ОРГАНИЗАЦИИ)

- Для кого:
  - государственных органов
  - организаций, в том числе субъектов КИИ
- Для чего:
  - создание основы для разработки детальных регламентов и стандартов по управлению уязвимостями с учетом особенностей функционирования органов (организаций) и организация взаимодействия между структурными подразделениями органов (организаций) по вопросам устранения уязвимостей



ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ
И ЭКСПОРТНОМУ КОНТРОЛЮ

Утвержден ФСТЭК России
17 мая 2023 г.

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

**РУКОВОДСТВО
ПО ОРГАНИЗАЦИИ ПРОЦЕССА УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ В ОРГАНЕ (ОРГАНИЗАЦИИ)**

2023

Цикл управления уязвимостями

Распределение обязанностей

- Специалисты по информационной безопасности:
  - Мониторинг уязвимостей и оценка их применимости
  - Оценка уязвимостей
  - Определение методов и приоритетов устранения уязвимостей
  - Разработка и реализация компенсирующих мер защиты информации
  - Контроль устранения уязвимостей
  - Разработка предложений по улучшению процесса управления уязвимостями
- Системные администраторы:
  - Устранение уязвимостей
  - Разработка и реализация компенсирующих мер защиты информации

1. МОНИТОРИНГ УЯЗВИМОСТЕЙ И ОЦЕНКА ИХ ПРИМЕНИМОСТИ

- Анализ информации об уязвимости
- Оценка применимости уязвимости
- Принятие решений на получение дополнительной информации
- Постановка задачи на сканирование объектов
- Сканирование объектов
- Оценка защищенности

Источники информации об уязвимостях

- БДУ ФСТЭК России: https://bdu.fstec.ru/
- NIST NVD: https://nvd.nist.gov/
- Chinese National Vulnerability Database (CNNVD): https://www.cnvd.org.cn/
- Debian GNU/Linux Security Bug Tracker

https://security-tracker.debian.org/tracker/

- Ubuntu CVE Tracker

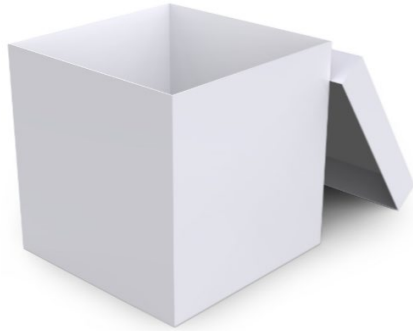
https://people.canonical.com/~ubuntu-security/cve/

- RHEL/CentOS Security Data https://www.redhat.com/security/data/metrics/

Подходы к тестированию защищенности и «ящики»

Red teaming

Сканирование на наличие уязвимостей



Анализ конфигурации

Комплексный подход: комбинация рассмотренных подходов и приемов злоумышленников

идентификация целевых сетевых узлов

- сбор информации о внешних ресурсах в Интернет
- сканирование сети
- согласование перечня с заказчиком

поиск уязвимостей

- с помощью сканеров
- вручную (по баннерам, ошибки конфигурации)

эксплуатация уязвимостей и проведение атак

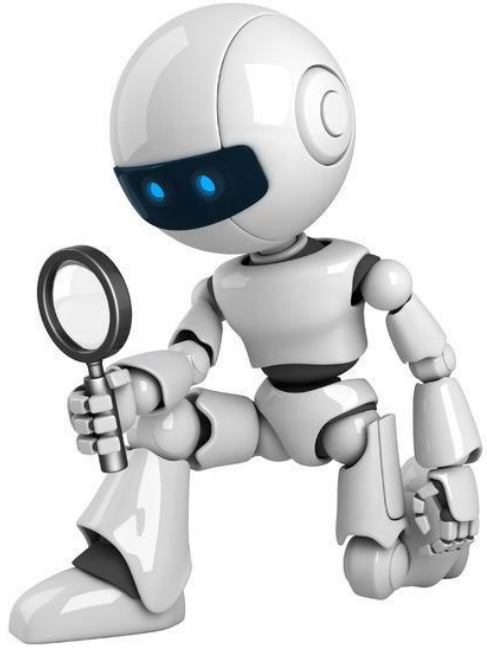
- подбор паролей
- перехват трафика
- запуск эксплойтов
- и т.д.

расширение привилегий и зоны влияния

- запуск локальных эксплойтов
- использование собранной информации для доступа к другим системам

Поиск уязвимостей

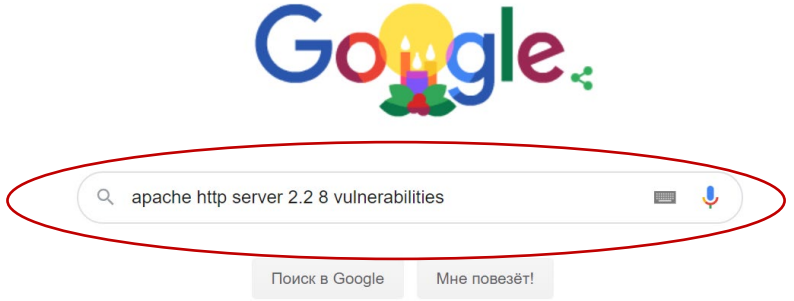
Ручной



С помощью сканеров

Технология ручного поиска уязвимостей

Apache HTTP Server 2.2.8



Apache » Http Server » 2.2.8 : Security Vulnerabilities (Execute Code)

Cpe Name:*cpe:/a:apache:http_server:2.2.8*
CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending
Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2013-1862	310		Exec Code	2013-06-10	2017-09-18	5.1	None	Remote	High	Not required	Partial	Partial	Partial

mod_rewrite.c in the mod_rewrite module in the Apache HTTP Server 2.2.x before 2.2.25 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to execute arbitrary commands via an HTTP request containing an escape sequence for a terminal emulator.

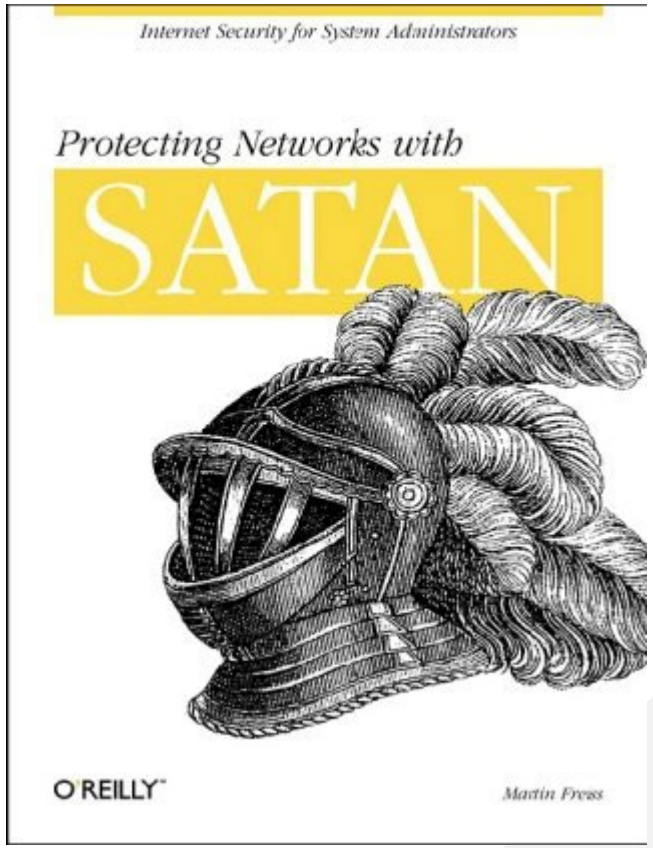
2	CVE-2010-0425			Exec Code	2010-03-05	2018-10-30	10.0	None	Remote	Low	Not required	Complete	Complete	Complete

modules/arch/win32/mod_isapi.c in mod_isapi in the Apache HTTP Server 2.0.37 through 2.0.63, 2.2.0 through 2.2.14, and 2.3.x before 2.3.7, when running on Windows, does not ensure that request processing is complete before calling isapi_unload for an ISAPI .dll module, which allows remote attackers to execute arbitrary code via unspecified vectors related to a crafted request, a reset packet, and "orphaned callback pointers."

Total number of vulnerabilities : **2** Page : 1 (This Page)

Первый сканер уязвимостей

- Релиз первого сканера уязвимостей SATAN (Security Administration Tool) состоялся в 5 апреля 1995
- Типы уязвимостей, которые он обнаруживал:
  - Файловые системы NFS, экспортируемые на произвольные хосты
  - Файловые системы NFS, экспортируемые в непривилегированные программы
  - Файловые системы NFS, экспортируемые через portmapper
  - Доступ к файлам с паролями NIS с произвольных хостов
  - Старые (т.е. до версии 8.6.10) версии sendmail
  - Доступ к REXD с произвольных хостов
  - отключен контроль доступа к X-серверу
  - доступ к произвольным файлам через TFTP
  - удаленный доступ к оболочке с произвольных хостов
  - доступный для записи домашний каталог анонимного FTP
- Написан на Perl и shell-скриптах

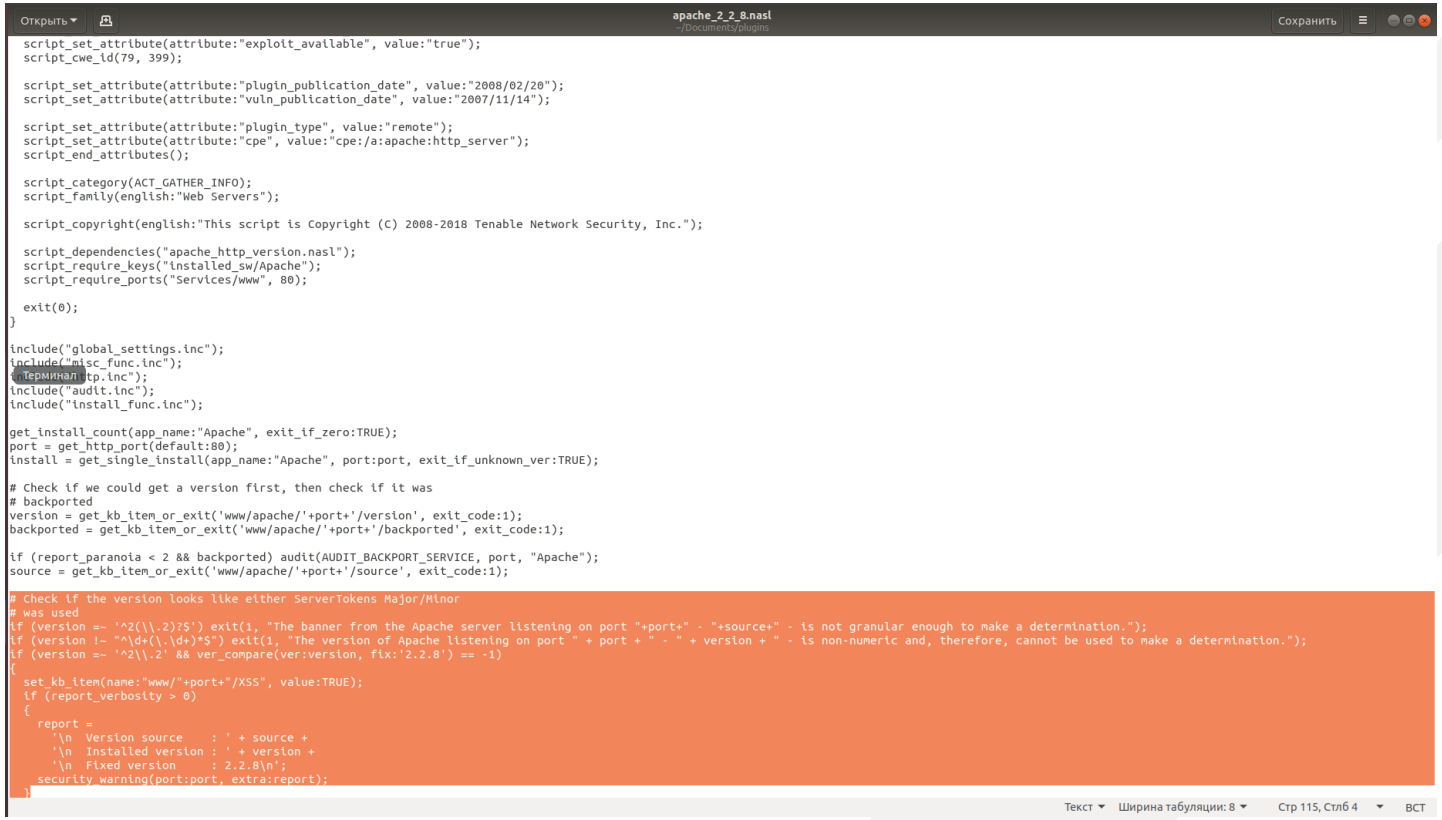


Сайт: http://www.porcupine.org/satan/

Запуск скриптов для проверок до сих пор применяется

Nessus Attack Scripting Language

Nmap Scripting Engine



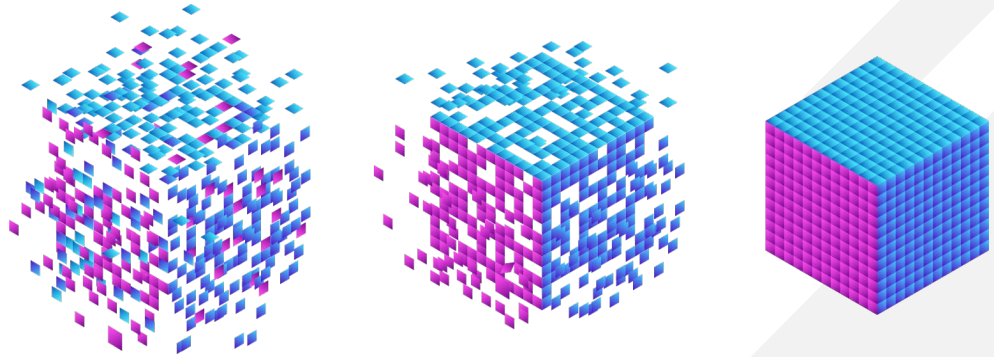

```
  script_set_attribute(attribute:"exploit_available", value:"true");
  script_cwe_id(79, 399);

  script_set_attribute(attribute:"plugin_publication_date", value:"2008/02/20");
  script_set_attribute(attribute:"vuln_publication_date", value:"2007/11/14");

  script_set_attribute(attribute:"plugin_type", value:"remote");
  script_set_attribute(attribute:"cpe", value:"cpe:/a:apache:http_server");
  script_end_attributes();

  script_category(ACT_GATHER_INFO);
  script_family(english:"Web Servers");

  script_copyright(english:"This script is Copyright (C) 2008-2018 Tenable Network Security, Inc.");

  script_dependencies("apache_http_version.nasl");
  script_require_keys("installed_sw/Apache");
  script_require_ports("Services/www", 80);

  exit(0);
}

include("global_settings.inc");
include("misc_func.inc");
include("http.inc");
include("audit.inc");
include("install_func.inc");

get_install_count(app_name:"Apache", exit_if_zero:TRUE);
port = get_http_port(default:80);
install = get_single_install(app_name:"Apache", port:port, exit_if_unknown_ver:TRUE);

# Check if we could get a version first, then check if it was
# backported
version = get_kb_item_or_exit('www/apache/'+port+'/version', exit_code:1);
backported = get_kb_item_or_exit('www/apache/'+port+'/backported', exit_code:1);

if (report_paranoia < 2 && backported) audit(AUDIT_BACKPORT_SERVICE, port, "Apache");
source = get_kb_item_or_exit('www/apache/'+port+'/source', exit_code:1);

# Check if the version looks like either ServerTokens Major/Minor
# was used
if (version =~ '^2(\\.2)?$') exit(1, "The banner from the Apache server listening on port "+port+" - "+source+" - is not granular enough to make a determination.");
if (version !~ "^\d+(\.\d+)*$") exit(1, "The version of Apache listening on port " + port + " - " + version + " - is non-numeric and, therefore, cannot be used to make a determination.");
if (version =~ '^2\\.2' && ver_compare(ver:version, fix:'2.2.8') == -1)
{
  set_kb_item(name:"www/"+port+"/XSS", value:TRUE);
  if (report_verbosity > 0)
  {
    report =
      '\n  Version source    : ' + source +
      '\n  Installed version : ' + version +
      '\n  Fixed version     : 2.2.8\n';
    security_warning(port:port, extra:report);
  }
```

Проблемы скриптового подхода

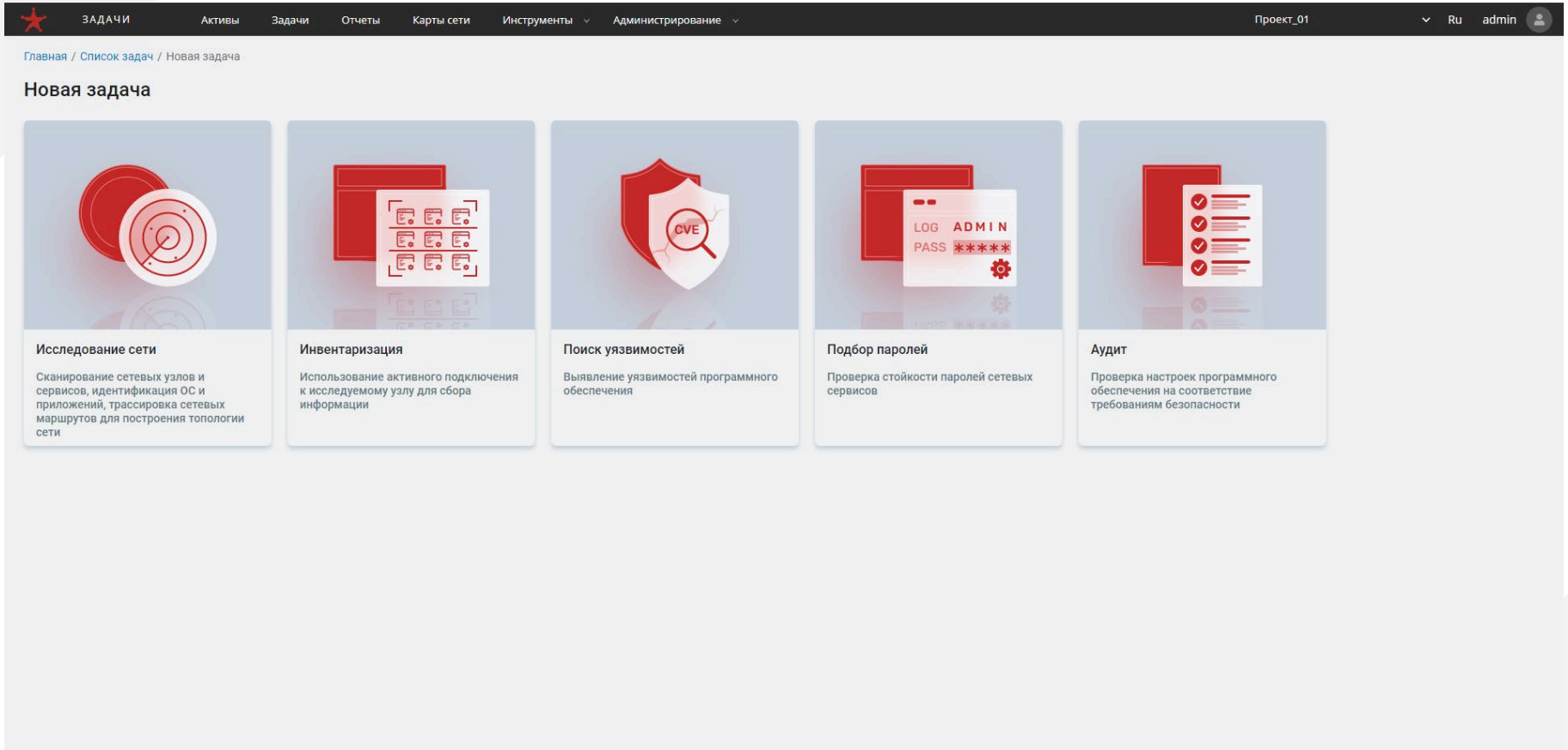
- Нужно поддерживать несколько десятков тысяч плагинов/скриптов, выявляющих уязвимости.
- Сканирование одного узла может занимать десятки минут.

Современный подход: использование агрегированной базы данных уязвимостей

- БДУ ФСТЭК России
- NIST National Vulnerability Database
- База обновлений Windows
- RHEL/CentOS Security Data
- Ubuntu CVE Tracker
- Debian GNU/Linux Security Bug Tracker
- …

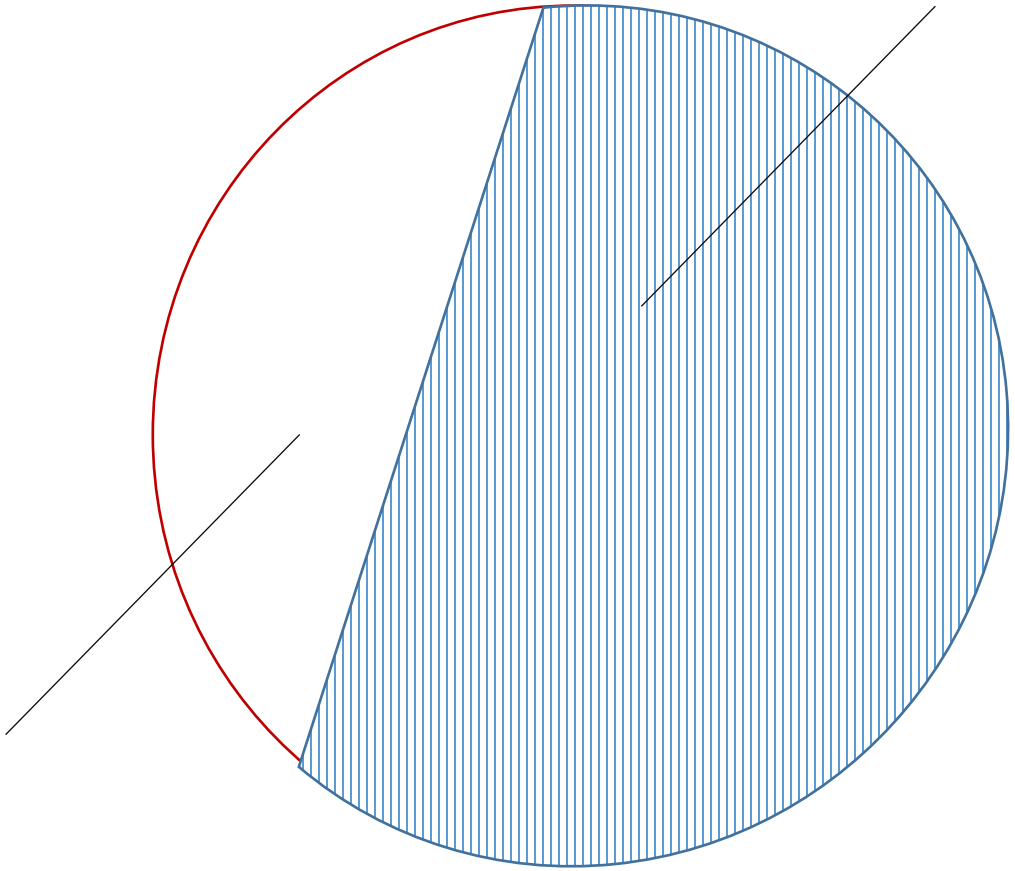


Сканер-ВС 6: основные функции



Источник информации о версиях: сетевое сканирование и инвентаризация

Все программные пакеты, включая локальные.
Требуется административный доступ по SSH/WinRM.



Сетевые сервисы:
требуется только доступ по сети

2. ОЦЕНКА УЯЗВИМОСТЕЙ

- Получение информации об объектах, подверженных уязвимости
- Определение уровня опасности уязвимости
- Определение влияния на информационные системы
- Расчет критичности уязвимости

От чего зависит наше восприятие опасности уязвимости?

- Внешние факторы:
  - Оценка уязвимости по CVSS
  - Оценка потенциальной возможности эксплуатации (EPSS)
  - Наличие опубликованных эксплойтов
- Внутренние факторы:
  - Доступность актива извне
  - Особенности ИТ-инфраструктуры
  - Особенности конфигурации систем
  - Критичность активов с точки зрения бизнеса

Степень опасности уязвимости

- Common Vulnerability Scoring System (CVSS) — это открытый стандарт, используемый для расчета количественной оценки степени опасности.
- При расчете учитываются такие факторы, как наличие эксплойта, возможность удаленной эксплуатации, необходимость авторизации, возможные последствия.
- Калькуляторы для расчета CVSS 2/3/3.1: https://bdu.fstec.ru/calc

Оценка по CVSS v4: CVE-2022-41741

CVSS v4 Score: Base 7.3

Metric	Value	Comments
Attack Vector	Local	У атакующего должен быть интерактивный доступ к системе
Attack Complexity	Low	Специальных условий и знаний не требуется
Attack Requirements	Present	Для успешной эксплуатации этой уязвимости необходимо выполнить множество условий, требующих сбора информации и подготовки цели.
Privileges Required	Low	Атакующий должен иметь возможность поместить файл в корневой каталог NGINX.
User Interaction	None	Взаимодействия с пользователем не требуется
Vulnerable System Confidentiality	High	Злоумышленник может выполнить произвольный код на уязвимой системе с повышенными привилегиями.
Vulnerable System Integrity	High	Злоумышленник может выполнить произвольный код на уязвимой системе с повышенными привилегиями.
Vulnerable System Availability	High	Злоумышленник может выполнить произвольный код на уязвимой системе с повышенными привилегиями.
Subsequent System Confidentiality	None	Это не повлияет на последующую конфиденциальность системы.
Subsequent System Integrity	None	Это не повлияет на последующую целостность системы.
Subsequent System Availability	None	Это не повлияет на последующую доступность системы.

Определение степени опасности уязвимости

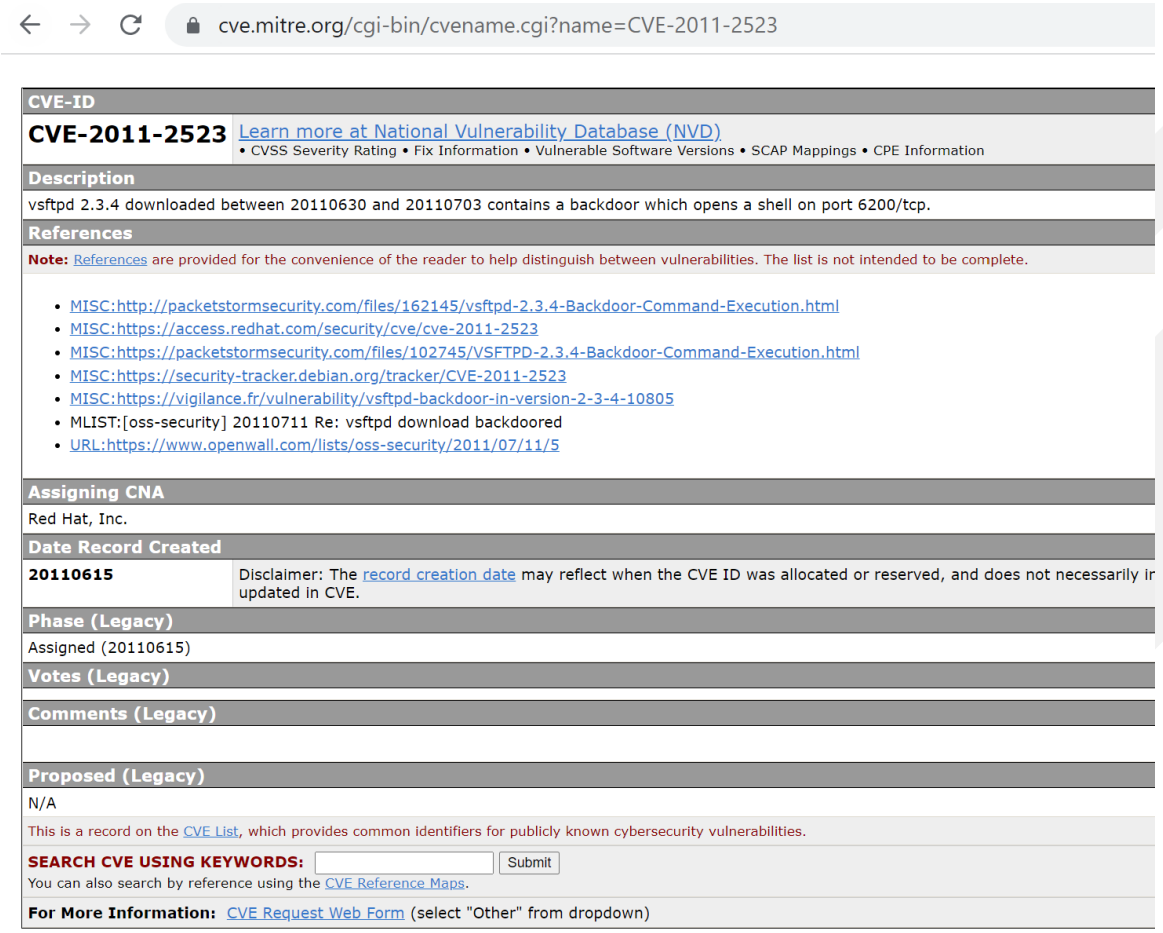
- CVSSv2:
  - Низкая (Low) – 0.0 – 3.9
  - Средняя (Medium) – 4.0 – 6.9
  - Высокая (High) – 7.0 – 10.0

- CVSSv3/v3.1/v4:
  - Не определен (None) – 0.0
  - Низкая (Low) – 0.1 – 3.9
  - Средняя (Medium) – 4.0 – 6.9
  - Высокая (High) 7.0 – 8.9
  - Критическая (Critical) – 9.0 – 10.0

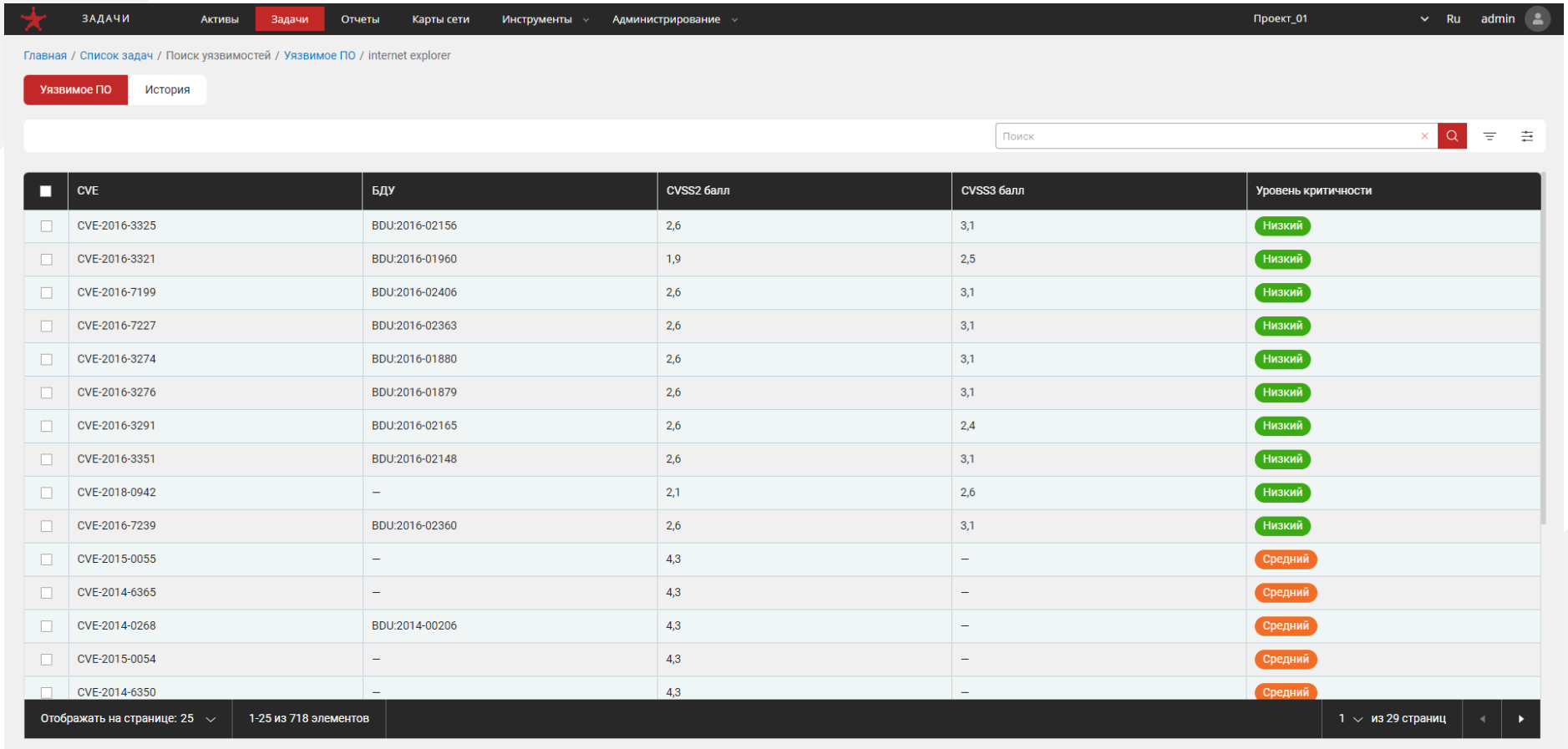
CVE

- CVE (Common Vulnerabilities and Exposures) — база данных общеизвестных уязвимостей информационной безопасности. Каждой уязвимости присваивается идентификационный номер вида CVE-год-номер, описание и ряд общедоступных ссылок с описанием.

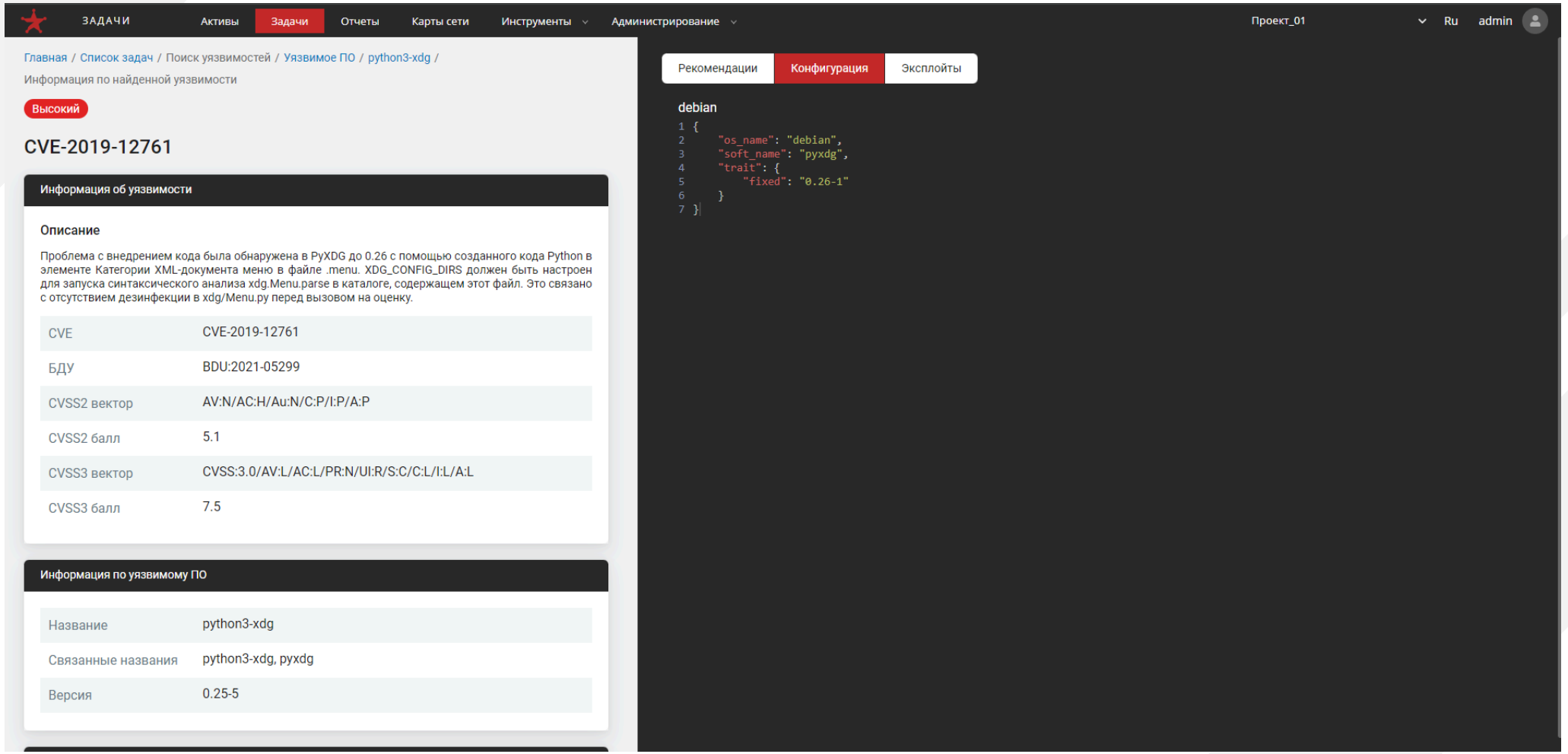
- https://www.cve.org/



Идентификаторы CVE и BDU в Сканер-ВС 6



Карточка уязвимости в Сканер-ВС 6



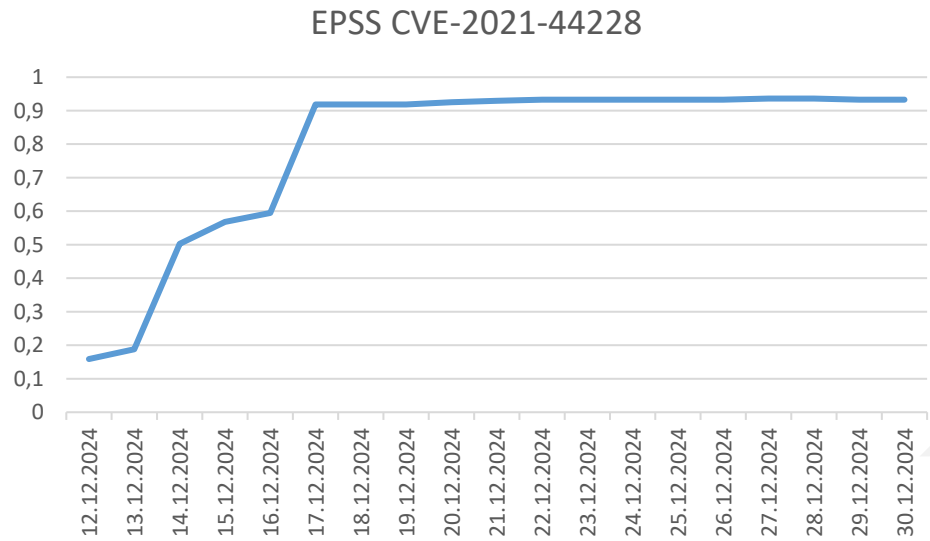
EPSS

- EPSS предоставляет возможности для эффективного управления уязвимостями на основе данных. Основана основана на данных и использует текущую информацию об угрозах из CVE и реальные данные об эксплойтах.
- Модель EPSS выдает оценку вероятности от 0 до 1 (от 0 до 100 %), где чем выше оценка, тем больше вероятность того, что уязвимость будет использована.

Как работает модель EPSS?

1. Сбор информации об уязвимостях из различных источников.
2. Сбор информации об ежедневной активности по эксплуатации.
3. Обучение модели: выявление взаимосвязей между информацией об уязвимостях и активностью по эксплуатации.
4. Измерение производительности модели и повторение 3 шага для оптимизации модели.
5. Ежедневное обновление информации об уязвимостях (шаг 1) и использование модели (шаг 3) для получения ежедневных оценок вероятности эксплуатации в течение следующих 30 дней для каждого опубликованного CVE.

Уязвимость Log4shell



24.11.21 — Chen Zhaojun Обнаруживает уязвимость

26.11.21 — Резервирование идентификатора CVE-2021-44228

06.12.21 — Выпуск Log4j 2.15.0, в которой закрыта уязвимость

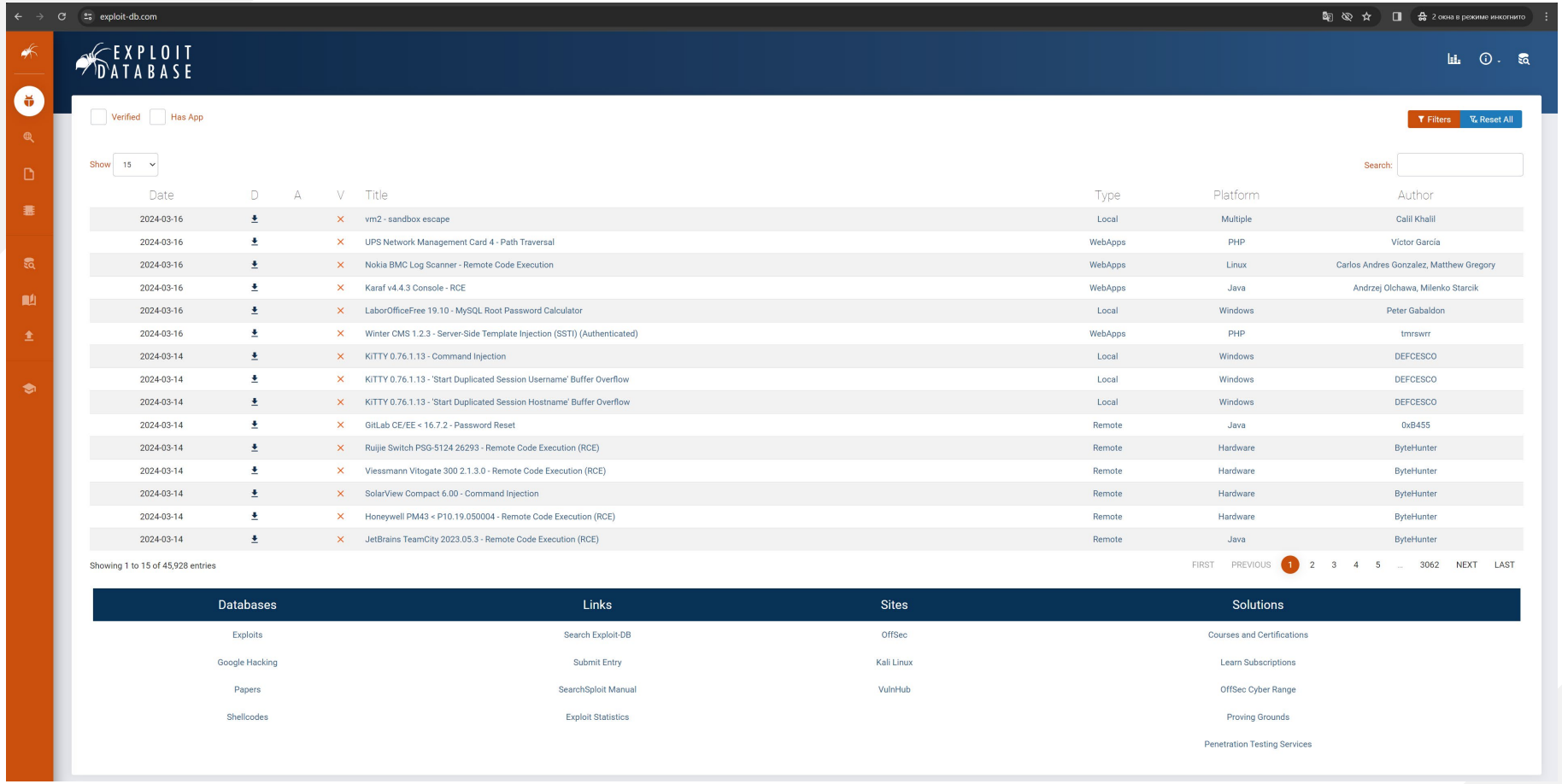
09.12.21 — Публикация в Твиттере

10.12.21 — Публикация информации об уязвимости CVE-2021-44228

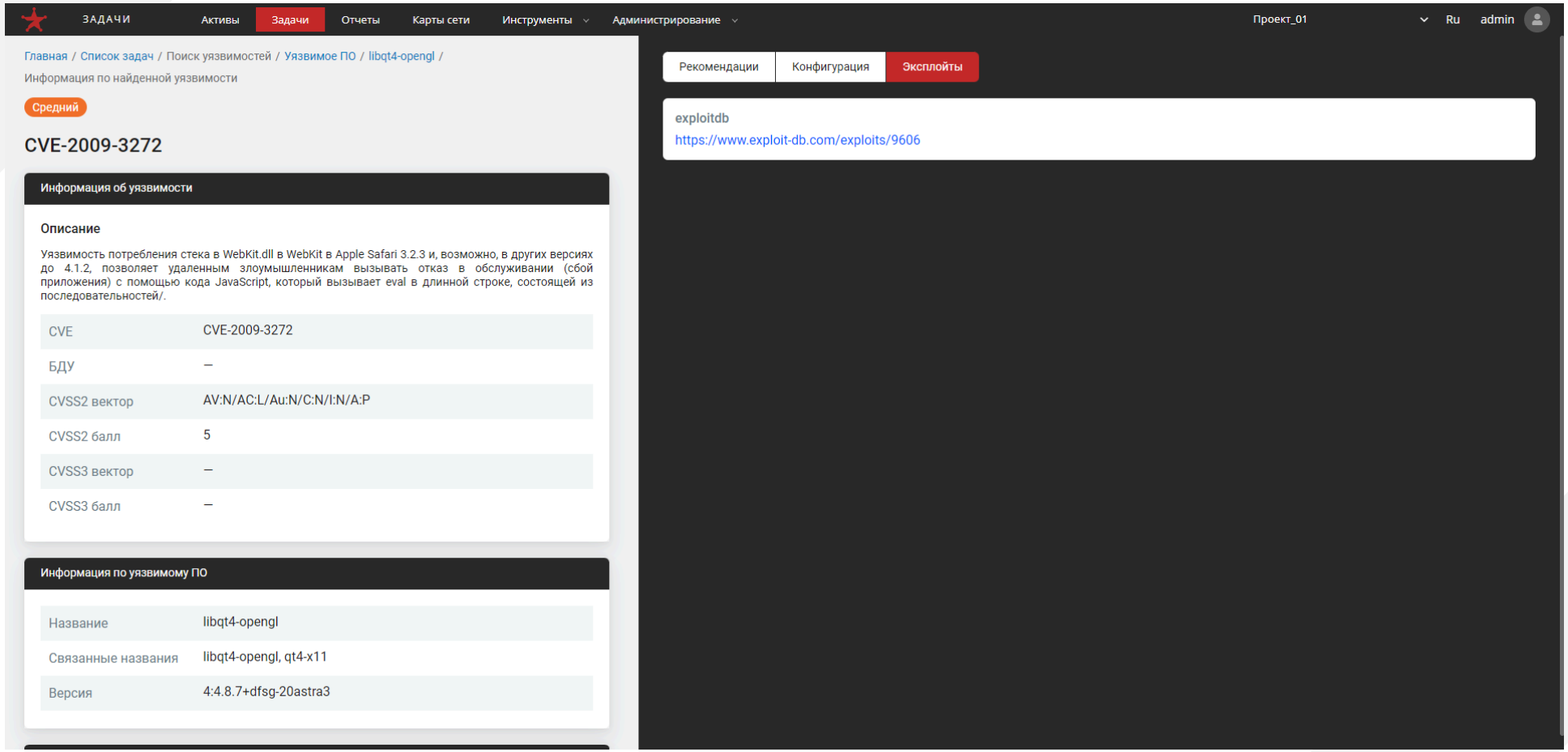
12.12.21 — Появилась оценка EPSS

17.12.21 — Повышение уровня опасности до критического, так как 2.15.0 все уязвимы.

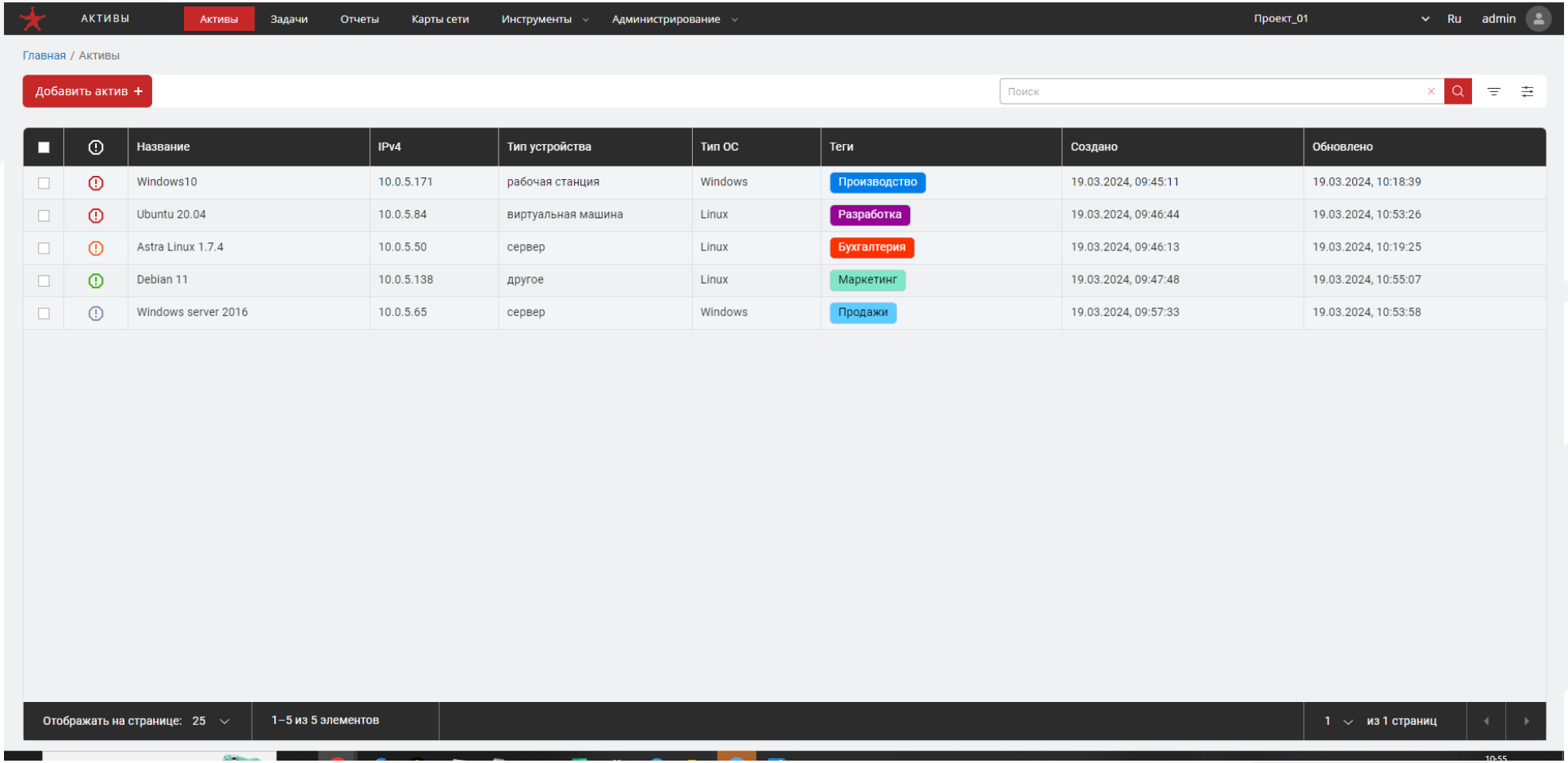
Где публикуются эксплойты?



Информация о доступных эксплойтах



Теги и критичность



3. ОПРЕДЕЛЕНИЕ МЕТОДОВ И ПРИОРИТЕТОВ УСТРАНЕНИЯ УЯЗВИМОСТЕЙ

- Определение приоритетности устранения уязвимостей
- Определение методов устранения уязвимостей
- Принятие решения о срочной установке обновлений
- Создание заявки на срочную установку обновления
- Принятие решения о срочной реализации компенсирующих мер защиты информации
- Создание заявки на установку обновления
- Создание заявки на реализацию компенсирующих мер защиты информации

4. УСТРАНЕНИЕ УЯЗВИМОСТЕЙ

- Согласование установки с руководством подразделения ИТ
- Тестирование обновления
- Установка обновления в тестовом сегменте
- Принятие решения об установке обновления
- Установка обновления
- Формирование плана установки обновлений
- Разработка и реализация компенсирующих мер защиты информации

Способы устранения уязвимостей

- Установка патча или новой версии
- Отключение сетевой службы, если есть возможность ее заменить или отказаться вовсе
- Ограничение доступа к уязвимому сервису или активу (например, ограничение по IP)
- Использование средств защиты, блокирующих эксплуатацию уязвимости (IPS, WAF, AV)

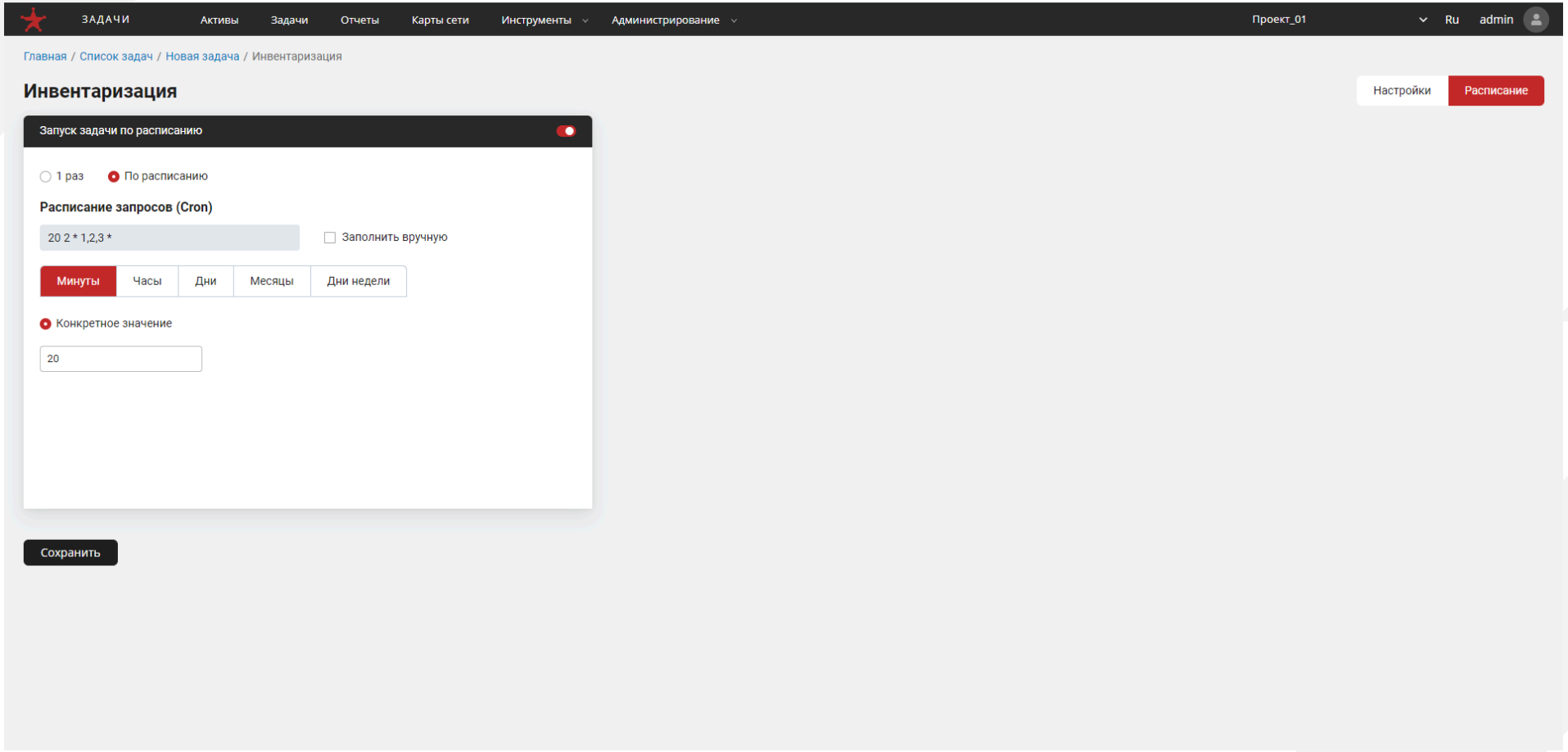
Рекомендуемые сроки устранения уязвимостей

- критический уровень опасности до 24 часов
- высокий уровень опасности – до 7 дней
- средний уровень опасности – до 4 недель
- низкий уровень опасности – до 4 месяцев

5. Контроль устранения уязвимостей

- Принятие решения о способе контроля
- Проверка объектов на наличие уязвимостей
- Оценка защищенности
- Выявление отклонений и неисполнений
- Разработка предложений по улучшению процесса управления уязвимостями

Запуск по расписанию и отправка событий в SIEM



Выводы

- Процессы управления уязвимостями достаточно хорошо проработаны методически.
- Инструментарий для ключевого процесса по выявлению уязвимостей разработан и доступен.
- Ключевым навыком экспертов является приоритезация уязвимостей.

Спасибо!

Сканер-ВС 6 в телеграм