

Описание функциональных характеристик программного обеспечения

VULNUM

АО «Сайбер ОК»
г. Москва, 2026 год

АННОТАЦИЯ

Настоящий документ предназначен для описания функциональных характеристик программного обеспечения VULNUM (далее — Система) в части базовых функциональностей и модулей:

- Сбор информации об описаниях уязвимостей;
- Сбор информации о методах эксплуатации уязвимостей
- Расчет метрик угроз для уязвимостей;
- Административная панель;
- Веб-интерфейс Системы.

ОГЛАВЛЕНИЕ

Аннотация.....	2
Оглавление	3
1 Термины и определения.....	4
2 Цели, назначение и области использования системы.....	5
3 Основные технические решения	6
3.1 Решения по структуре и архитектуре	6
3.2 Описание функциональные характеристик Системы.....	8
3.2.1 Сбор данных	8
3.2.2 Хранение данных	8
3.2.3 Функции веб-интерфейса пользователя	8
3.2.4 Функции веб-интерфейса администратора Системы	10
3.3 Общие сведения по программно-аппаратному обеспечению Системы	10
ПРИЛОЖЕНИЕ А. Каталог основных пользовательских интерфейсов Системы.....	11

1 ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Таблица 1. Термины и определения

№	Термин/Сокращение	Определение/Расшифровка
1.	ИБ	Информационная безопасность
2.	Веб-интерфейс	Графический интерфейс пользователя
3.	РРПО	Реестр российского программного обеспечения
4.	Application Programming Interface (API)	Механизм, обеспечивающий интеграционное взаимодействие внутри компонентов системы, а также с внешними приложениями и системы
5.	Computer Emergency Response Teams (CERT)	Группа экспертов по компьютерной безопасности, занимающаяся сбором информации об инцидентах, их классификацией и нейтрализацией

2 ЦЕЛИ, НАЗНАЧЕНИЕ И ОБЛАСТИ ИСПОЛЬЗОВАНИЯ СИСТЕМЫ

Цели создания и области применения Системы:

- Сбор справочной информации об известных уязвимостях в различных видах программного обеспечения ;
- Сбор информации о способах эксплуатации уязвимостей в различных видах программного обеспечения;
- Сбор информации об упоминании уязвимостей в социальных сетях
- Расчет метрик угроз для каждой уязвимости.

Внедрение и использование Системы позволит обеспечить выполнение следующих задач:

- поиск, фильтрация, просмотр актуальных данных об уязвимостях существующих в различных видах и версиях программного обеспечения;
- анализ активности в социальных сетях по уязвимостям;
- оценка рисков эксплуатации уязвимости в настоящее время.

Система предназначена для следующих ключевых пользователей:

- **Администратор Системы** — сотрудник оператора Системы, обладающий неограниченными полномочиями по действиям в Системе (добавление/блокировка/настройка пользователей Системы, настройка и запуск задач по сбору данных, настройка справочников);
- **Оператор** — пользователь, осуществляющий актуализацию сведений об уязвимостях.
- **Лицензированный пользователь** — пользователь, обладающий лицензией и, в зависимости от типа лицензии, имеющий полномочия на просмотр данных по уязвимостям и способам их эксплуатации.

3 ОСНОВНЫЕ ТЕХНИЧЕСКИЕ РЕШЕНИЯ

3.1 Решения по структуре и архитектуре

Система разработана на базе архитектуры клиент-серверного веб-приложения, поддерживает технологию тонкого веб-клиента для доступа к сервисам серверной части Системы.

Система состоит из серверной части и веб-интерфейсов (см. Рисунок 1):

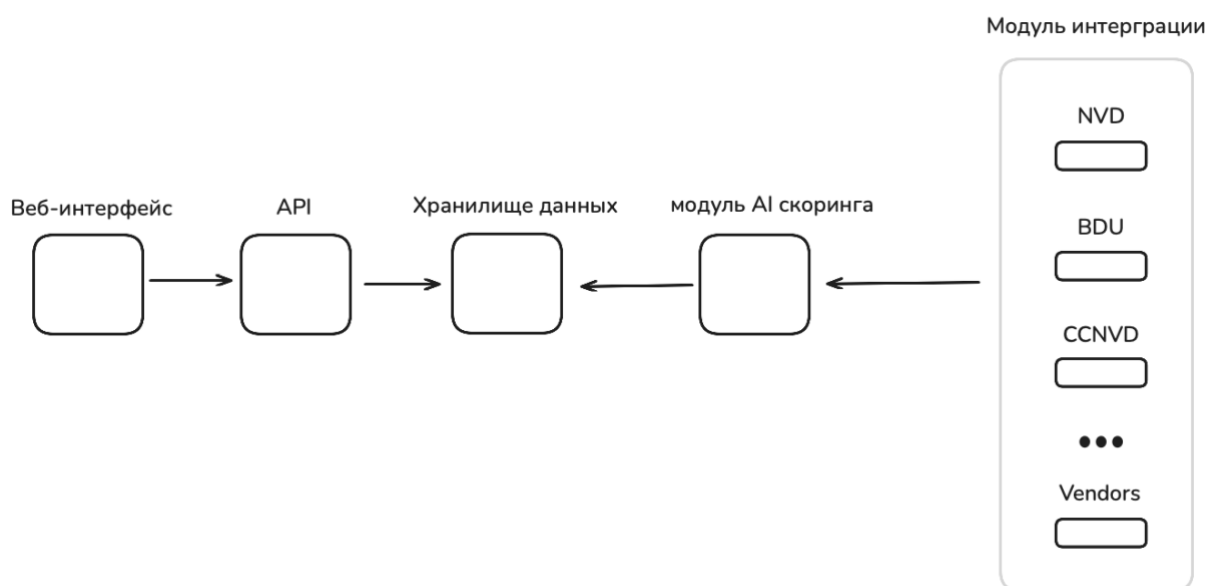


Рисунок 1. Архитектура Системы

Система включает компоненты:

— **Веб-интерфейс** — набор веб-страниц и веб-сервисов, которые реализуют функции Системы, предназначенные для пользователей Системы, в части доступа к просмотру, фильтрации и анализу данных об уязвимостях;

— **Хранилище данных** — базы данных для хранения данных уязвимостей, способах их эксплуатации и справочных данных с целью использования их для отображения в веб-интерфейсе Системы.

— **Модуль интеграции** — подсистема, включающая набор программных компонентов, реализующих внутреннюю функциональность в части логики работы веб-сервисов, алгоритмов сбора данных из различных источников и их сохранения в Хранилище данных;

— **Модуль AI скоринга** – подсистема производящая расчет метрик угроз для уязвимостей на основании собранных данных

— **API** — набор программных компонентов, предназначенных для взаимодействия через API между компонентами Системы.

3.2 Описание функциональные характеристик Системы

3.2.1 Сбор данных

Функциональность реализована с целью сбора, обогащения и агрегации данных об уязвимостях, способах их эксплуатации и упоминаниях в социальных сетях для составления базы знаний об уязвимостях.

Сбор данных реализуются в подсистеме «Модуль интеграции». Сбор данных осуществляется в соответствии с настройками конфигурации системы для каждого источника данных.

Источники данных используемые в системе:

- Банк данных угроз безопасности информации (БДУ, РФ)
- Национальная база данных уязвимостей (National Vulnerability Database, США)
- China National Vulnerability Database (CCNVD, Китай)
- Вендоры программного обеспечения: Астра линукс, Ubuntu, RedHat, Centos и другие

3.2.2 Хранение данных

Хранение данных об уязвимостях и данных справочников осуществляется в хранилище данных Системы. В Системе хранятся следующие виды данных:

- Информация из национальных баз данных уязвимостей, бюллетени безопасности вендоров;
- Информация о способах устранения уязвимости
- Информация о существующих эксплоитах и ссылки на них
- Информация о способах детектирования уязвимостей
- Информация об истории упоминания уязвимости в социальных сетях

3.2.3 Функции веб-интерфейса пользователя

Веб-интерфейс включает пользовательские интерфейсы Системы, предназначенные для поиска, фильтрации, просмотра и анализа информации, накопленной в Системе.

Веб-интерфейс обеспечивает выполнение следующих задач:

- Поиск информации об уязвимостях;
- Просмотр информации об уязвимости;
- Редактирование информации об уязвимости;

3.2.3.1 Авторизация в веб-интерфейсе

Авторизация в Веб-интерфейсе должна осуществляться после ввода логина и пароля на странице авторизации и нажатию на кнопку «Войти».

После авторизации в Веб-интерфейсе должен осуществляться переход к главной странице, содержащей функцию гибкого поиска по хостам.

3.2.3.2 Гибкий поиск и фильтрация данных

На главной странице пользовательского веб-интерфейса Системы реализован поиск информации об уязвимостях по параметрам:

- Идентификатор уязвимости;
- Оценка уровня угрозы (cvss.BaseScore, cvss.TemporalScore);
- Признак наличия эксплоита;
- Вектор атаки;
- Названию и версии программного обеспечения;
- Признак наличия способов детектирования уязвимости;
- Оценка степени риска уязвимости: Critical, High, Medium, Low;

В гибком поиске реализована возможность объединения запросов булевыми операторами, представляющими собой последовательность условий с целью определения нужных критериев поиска.

На странице гибкого поиска выводится информация о доступных для поиска параметрах/критериях.

В результатах поиска отображается список подходящих под критерии поиска со следующими данными для каждой уязвимости:

- Идентификатор уязвимости или бюллетеня
- Дата первичной публикации
- Дата последнего обновления
- Краткое описание уязвимости
- Метрики уровня угрозы: CVSS, EPSS, CybVSS, RealWordDangerScore
- Количество упоминаний уязвимости в социальных сетях
- Количество эксплоитов
- Распространенность (примерное количество сервисов в Интернет , на которых уязвимость потенциально может быть эксплуатирована)

3.2.3.3 Отображение информации об уязвимости

В Веб-интерфейсе Системы реализовано отображение информации об отдельной уязвимости, в этом случае доступны следующие данные:

- Подробное описание уязвимости на русском и английском языке;
- Ссылки на документы вендоров по данной уязвимости
- Упоминания уязвимости в социальных сетях
- Метрики угрозы для уязвимости
- История изменений уязвимости
- Конфигурации CPE, которые затрагивает данная уязвимость
- Связанное уязвимости и бюллетени
- Ссылки на внешние источники данных по уязвимости
- Шаблоны для детектирования уязвимости

3.2.3.4 Редактирование информации об уязвимости

Система позволяет как редактировать данные об уязвимости, так и создавать новые уязвимости со специальными идентификаторами СОК-XXXX-YYYYY для еще незарегистрированных уязвимостей.

Все изменения сохраняются в истории редактирований и могут быть просмотрены администратором

3.2.4 Функции веб-интерфейса администратора Системы

В части администрирования в Системе реализованы функции:

- Управление пользователями
- Управление справочниками
- Просмотр статистики
- Управление фильтрами уведомлений

3.3 Общие сведения по программно-аппаратному обеспечению Системы

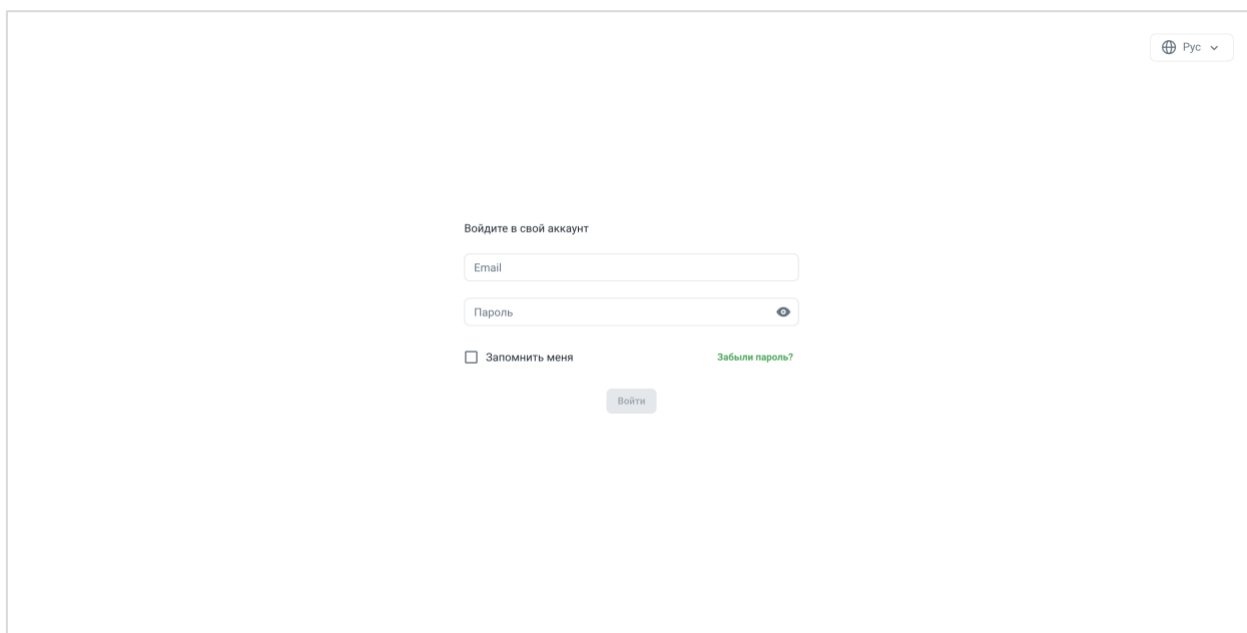
Модули Системы реализованы на базе операционной системы семейства Linux.

СУБД удовлетворяет требованиям импортозамещения.

Версии всего используемого системного программного обеспечения удовлетворяют требованиям информационной безопасности согласно классу защищенности Системы.

При создании Системы использовалось российское программное обеспечение и программные решения, построенные на базе свободного программного обеспечения.

ПРИЛОЖЕНИЕ А. Каталог основных пользовательских интерфейсов Системы



The screenshot displays a login interface within a web application. In the top right corner, there is a language selector button labeled "Рус" with a dropdown arrow. The main heading "Войдите в свой аккаунт" (Log in to your account) is centered. Below it are two input fields: "Email" and "Пароль" (Password), the latter featuring a toggle icon for password visibility. A checkbox labeled "Запомнить меня" (Remember me) is positioned to the left of a green link "Забыли пароль?" (Forgot password?). At the bottom center is a "Войти" (Log in) button.

Рисунок 2. Экран авторизации в web-приложении Системы

mentions.count:">0 by 7 days"

Найти

Добавить уязвимость/Мисskonфиг

Трендовые

Высокая оценка

Высокий EPSS

Часто упоминаются

Эксплуатируемые

1845 уязвимостей и мисskonфигураций из 11 источников

Уязвимостей и мисskonфигураций на странице25

1

2

3

4

5

Следующая

Дата обновленияДата публикацииBase ScoreКоличество упоминанийВажные упоминания↓EPSSCYBVSS

☐ Просмотрено

☐ Для исследования

Опубликовано25.09.2025Обновлено26.09.2025Внедрено30.09.2025, 07:25E61: 18.09-01.10

☐ CVE-2025-20333

EPSS 0.010

CybvSS 486.3

Real World Danger Score 5.0

A vulnerability in the VPN web server of Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) Software could allow an authenticated, remote attacker to execute arbitrary code on an...

Упоминаний61

Эксплоиты1

Распространенность0

Ссылки2

CVSS 3.1

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Base Score: 9.9Temporal Score: 9.9Environmental Score: 10Exploitability Score: 3.1Impact Score: 6

cpe:2.3:a:cisco:firepower_threat_defense:*:*:*:*:* + ещё 2

KEYadaptive_security_appliance_softwareciscocisco:adaptive_security_appliance_softwarecisco:firepower_threat_defensefirepower_threat_defense

Опубликовано19.09.2025Обновлено30.09.2025Просмотрено

☐ CVE-2025-10035

EPSS 0.811

CybvSS 211.7

Real World Danger Score 2.0

A deserialization vulnerability in the License Servlet of Fortra's GoAnywhere MFT allows an actor with a validly forged license response signature to deserialize an arbitrary actor-controlled object, possibly leading to command injection.

Упоминаний94

Эксплоиты0

Распространенность0

Ссылки2

CVSS 3.1

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Base Score: 10Temporal Score: 10Environmental Score: 10Exploitability Score: 3.9Impact Score: 6

cpe:2.3:a:fortra:goanywhere_managed_file_transfer:*:*:*:*:*

KEYfortrafortra:goanywhere_managed_file_transfergoanywhere_managed_file_transfer

Рисунок 3. Главный экран, поиск по уязвимостям

Уязвимости и миссконфигурации > CVE-2025-20333

CVE-2025-20333

https://nvd.nist.gov/vuln/detail/CVE-2025-20333

Загружено

25.09.2025, 19:12

Обновлено

26.09.2025, 18:02

Подробности

Упоминания

61

Конфигурации (CPEs)

Эксплоиты

1

История

RuEn

A vulnerability in the VPN web server of Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) Software could allow an authenticated, remote attacker to execute arbitrary code on an affected device. This vulnerability is due to improper validation of user-supplied input in HTTP(S) requests. An attacker with valid VPN user credentials could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as root, possibly resulting in the complete compromise of the affected device.

Ссылки

Ссылка	Ресурс
https://sec.cloudapps.cisco.com/security/center/resources/asa_ftd_continued_attacks	
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-webvpn-z5xP8EUB	

Статус

Внедрено

Ссылка на задачу #2570

Внедрено с

30.09.2025, 07:25

Исследователь

Roman Malov

Milestone

E61: 18.09-01.10

expertpriority:highresearch:mergedroosterthreatchecking

Base score (CVSS 3.1)

9.9

EPSS

0.010

Cybvss

486.3

Real world danger score

5.0

KEYVendor Advisory

CVSS 3.1

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Base Score

9.9

Temporal Score

9.9

Environmental Score

10

Exploitability Score

3.1

Impact Score

6

Base Score Metrics

Exploitability Metrics

Attack vector (AV)

NETWORK

Attack Complexity (AC)

LOW

Privileges Required (PR)

LOW

User Interaction (UI)

NONE

Scope (S)

CHANGED

Nuclei-шаблоны для определения уязвимости

> Cisco ASA and FTD Software - Information Disclosure Vulnerability

Тип

private

Точность

0.8

Урон

0.1

Теги

cvecve2020cve-2020cve-2020-3259ciscociscoasaciscoftd

Ссылки

cisco-adaptive_security_appliance_software-bannercheck-direct.yaml

Запросы в других системах (ASM)

Shodan

set-cookie: webvpn=;ssl.cert.subject.cn:"firepower"product:"Cisco ASA SSL VPN"

Rooster

http:"webvpn=" OR product.name:"cisco ssl"

Рисунок 4. Просмотр информации об уязвимости



CVE-2025-20333

<https://nvd.nist.gov/vuln/detail/CVE-2025-20333>

Загружено 25.09.2025, 19:12
Обновлено 26.09.2025, 18:02

Подробности Упоминания 61 Конфигурации (CPEs) Эксплоиты 1 История

Период упоминаний:

Все упоминания

cyberplace.social | Kevin Beaumont

02.10.2025, 16:09

My Cisco ASA firmware versions scan is now public: <https://github.com/GossiTheDog/scanning/blob/main/Cisco-ASA-firmware-updates-CVE-2025-20333-CVE-2025-20363-CVE-2025-20362.csv>Fields:IP,hostnames,FirmwareVersionKnown,FirmwareModifiedDate,ErrorsDates are UK date format - DD/MM/YYIf FirmwareModifiedDate is below */08/25 or */09/25, the device is vulnerable to #CyberWillyWave as the firmware was compiled August 2025 or later.New scan running now, results at weekend.It gives you a very good indication as to how regularly orgs patch, e.g.

bsky.app | GreyNoise

02.10.2025, 01:19

GreyNoise now has coverage for Cisco zero-days CVE-2025-20333 and CVE-2025-20362. Watch for exploit attempts in real-time:CVE-2025-20333 (Net-new): viz.greynoise.io/tags/cisco-a... (Updated tag): viz.greynoise.io/tags/cisco-a...

infosec.exchange | GreyNoise

02.10.2025, 01:09

GreyNoise now has coverage for Cisco zero-days CVE-2025-20333 and CVE-2025-20362. Watch for exploit attempts in real-time:CVE-2025-20333 (Net-new): <https://viz.greynoise.io/tags/cisco-asa-vpn-input-validation-cve-2025-20333-rce-attempt?days=1>CVE-2025-20362 (Updated tag): <https://viz.greynoise.io/tags/cisco-asa-directory-traversal-cve-2018-0296-and-cve-2025-20362-attempt#CiscoASA> #Cisco #ZeroDay #CiscoZeroDays #CVE202520333 #CVE202520362 #GreyNoise #ThreatIntel

bsky.app | キタきつね

02.10.2025, 00:59

Cisco ASAおよびFTDにおける複数の脆弱性（CVE-2025-20333、CVE-2025-20362）に関する注意喚起 #JPCERTCC (Oct 1) www.jpcert.or.jp/at/2025/at25...

infosec.exchange | Jeff Hall - PCI Guru :verified:

01.10.2025, 17:29

The flaws, tracked as CVE-2025-20333 and CVE-2025-20362, enable arbitrary code execution and access to restricted URL endpoints associated with VPN access. Both security issues can be exploited remotely without authentication. <https://www.bleepingcomputer.com/news/security/nearly-50-000-cisco-firewalls-vulnerable-to-actively-exploited-flaws/>

Рисунок 5. Просмотр информации об упоминании уязвимостей в социальных сетях



CVE-2025-20333

<https://nvd.nist.gov/vuln/detail/CVE-2025-20333>

Загружено 25.09.2025, 19:12
Обновлено 26.09.2025, 18:02

Подробности Упоминания 61 Конфигурации (CPEs) Эксплоиты 1 История

Matching CPE CPE List

Matches from NVD	Version from	To version
❌ cpe:2.3:o:cisco:adaptive_security_appliance_software:*:*:*:*:*	9.12 (included)	9.12.4.72 (excluded)
❌ cpe:2.3:o:cisco:adaptive_security_appliance_software:*:*:*:*:*	9.14 (included)	9.14.4.28 (excluded)
❌ cpe:2.3:o:cisco:adaptive_security_appliance_software:*:*:*:*:*	9.16 (included)	9.16.4.85 (excluded)
❌ cpe:2.3:o:cisco:adaptive_security_appliance_software:*:*:*:*:*	9.17.0 (included)	9.17.1.45 (excluded)
❌ cpe:2.3:o:cisco:adaptive_security_appliance_software:*:*:*:*:*	9.18 (included)	9.18.4.47 (excluded)
❌ cpe:2.3:o:cisco:adaptive_security_appliance_software:*:*:*:*:*	9.19 (included)	9.19.1.37 (excluded)
❌ cpe:2.3:o:cisco:adaptive_security_appliance_software:*:*:*:*:*	9.20 (included)	9.20.3.7 (excluded)
❌ cpe:2.3:o:cisco:adaptive_security_appliance_software:*:*:*:*:*	9.22 (included)	9.22.1.3 (excluded)
❌ cpe:2.3:a:cisco:firepower_threat_defense:*:*:*:*:*	7.0.0 (included)	7.0.8.1 (excluded)
❌ cpe:2.3:a:cisco:firepower_threat_defense:*:*:*:*:*	7.1.0 (included)	7.2.9 (excluded)
❌ cpe:2.3:a:cisco:firepower_threat_defense:*:*:*:*:*	7.3.0 (included)	7.4.2.4 (excluded)
❌ cpe:2.3:a:cisco:firepower_threat_defense:7.6.0:*:*:*:*	-	-

Рисунок 6. Просмотр информации о CPE соответствующих уязвимости

**CVE-2025-20333** <https://nvd.nist.gov/vuln/detail/CVE-2025-20333>

Загружено 25.09.2025, 19:12

Обновлено 26.09.2025, 18:02

Подробности Упоминания **61** Конфигурации (CPEs) Эксплоиты **1** История

Тип события	Источник изменения	Дата и время	Предыдущее значение	Новое значение
Изменен EPSS	epss	02.10.2025, 08:58	0.008	0.010
Изменен EPSS	epss	29.09.2025, 19:16	0.010	0.008
Создан первый PoC	nomi-sec/PoC-in-GitHub	28.09.2025, 04:16	-	https://github.com/callinston/CVE-2025-20333
Изменен EPSS	epss	27.09.2025, 19:41	0.014	0.010
Добавлена связанная уязвимость	BDU	27.09.2025, 01:13	-	BDU:2025-11706
Изменен EPSS	epss	26.09.2025, 19:11		0.014
Изменена уязвимость	NVD	26.09.2025, 18:02	-	-
Изменена уязвимость	NVD	26.09.2025, 17:02	-	-
Изменена уязвимость	NVD	26.09.2025, 04:02	-	-
Изменен RWDS	crowd	25.09.2025, 22:33	4	5
Изменена уязвимость	NVD	25.09.2025, 22:02	-	-
Изменен RWDS	crowd	25.09.2025, 20:53		4
Изменена базовая оценка	NVD	25.09.2025, 20:02		9.900
Изменена уязвимость	NVD	25.09.2025, 20:02	-	-
Добавлен в CISA KEV	cisa	25.09.2025, 19:32	-	-
Добавлено первое упоминание	crowd	25.09.2025, 19:12	-	https://cyberplace.social/@GossiTheDog/115265778831418980

Рисунок 7. Просмотр информации об истории изменений уязвимости

Nuclei-шаблоны для определения уязвимости

Cisco ASA and FTD Software - Information Disclosure Vulnerability

```
1 id: cisco-adaptive_security_appliance_software-bannercheck-direct
2
3 info:
4   name: Cisco ASA and FTD Software - Information Disclosure Vulnerability
5   author: plgvkr, roman.malov
6   severity: info
7   description: |
8     A vulnerability in the web services interface of Cisco Adaptive
9     Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD)
10    Software could allow an unauthenticated, remote attacker to retrieve memory
11    contents on an affected device, which could lead to the disclosure of
12    confidential information.
13    reference:
14      - https://nvd.nist.gov/vuln/detail/CVE-2020-3259
15      - https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory
16        sa-asaftd-info-disclose-9eJtycMB
17    classification:
18      cve-id:
19      cvss-score:
20      epss-score:
21      cpe:
22        cpe:2.3:o:cisco:adaptive_security_appliance_software:*:*:*:*:*
23        #- cpe:2.3:a:cisco:firepower_threat_defense_software:*:*:*:*:*
24        # The NVD shows a different cpe for firepower threat defense
25        (cpe:2.3:a:cisco:firepower_threat_defense:*:*:*:*:*)
26    metadata:
27      date: 26.09.2025
28      expiration_date: 26.09.2026
29      code_requirements:
30      additional_files:
31      nuclei_commandline:
32      bdu-id:
33      cok-id:
34      template_type: bannercheck-direct
35      verified: false
```

CVSS 3.1

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Base Score	9.9
Temporal Score	9.9
Environmental Score	10
Exploitability Score	3.1
Impact Score	6

Base Score Metrics

Exploitability Metrics

Attack vector (AV)	NETWORK
Attack Complexity (AC)	LOW
Privileges Required (PR)	LOW
User Interaction (UI)	NONE
Scope (S)	CHANGED

Развернуть

CWE-120

Buffer Copy without Checking Size of Input ('Clastic Buffer Overflow')

Рисунок 8. Экран просмотра информации по найденному хосту

Уязвимости > CVE-2025-20333 > Редактирование

CVE-2025-20333

Сохранить

Выйти без сохранения

Загружено

25.09.2025, 19:12

Обновлено

26.09.2025, 18:02

https://nvd.nist.gov/vuln/detail/CVE-2025-20333

Причина редактирования

Заголовок

Введите заголовок уязвимости

Описание

Ru

Уязвимость в веб-сервере VPN программного обеспечения Cisco Secure Firewall Adaptive Security Appliance (ASA) и Cisco Secure Firewall Threat Defense (FTD) может позволить аутентифицированному удалённому злоумышленнику выполнить произвольный код на уязвимом устройстве. Эта уязвимость вызвана некорректной проверкой данных, предоставленных пользователем в HTTP(S)-запросах.

En

A vulnerability in the VPN web server of Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) Software could allow an authenticated, remote attacker to execute arbitrary code on an affected device.

Рекомендации

Ru

En

Воспроизведения

Добавить воспроизведение

Шаги по исправлению

Добавить шаги по исправлению

Ссылки

https://sec.cloudapps.cisco.com/security/center/resources/asa_ftd_continued_attacks

×

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-we

×

EPSS

0.010

CybvSS ⓘ

486.3

Real world danger score ⓘ

5.0

KEV

Vendor Advisory

CVSS 4.0

CVSS 3.1

CVSS 3.0

CVSS 2.0

☒ Использовать метрику

Vector string

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Source

psirt@cisco.com

Type

Primary

Base Score Metrics

Exploitability Metrics

Attack vector (AV)

NETWORK

Attack complexity (AC)

LOW

Privileges required (PR)

LOW

User interaction (UI)

NONE

Scope (S)

CHANGED

Impact Metrics

Confidentiality impact (C)

HIGH

Integrity impact (I)

HIGH

Availability impact (A)

HIGH

Рисунок 9. Экран просмотра информации по найденному хосту, блок «Уязвимости» и блок «История»

Инструкции в случае развёртывания экземпляра ПО или удалённого доступа к инфраструктуре с развёрнутым экземпляром ПО

VULNUM

АО «Сайбер ОК»
г. Москва, 2026 год

АННОТАЦИЯ

Настоящий документ содержит инструкции по работе с программным обеспечением Vulnum для случаев:

- удалённого доступа к инфраструктуре с развёрнутым экземпляром ПО;
- развёртывания автономного экземпляра ПО (стенда).

Документ актуализирован по состоянию на август 2026 года и соответствует версии веб-интерфейса Vulnum v2, развёрнутой на демонстрационном стенде.

ОГЛАВЛЕНИЕ

Аннотация	2
Оглавление	3
1 Цели, назначение и области использования системы	5
2 Удалённый доступ к инфраструктуре с развёрнутым экземпляром ПО	6
2.1 Доступ к узлу по протоколу SSH	6
2.2 Вход в веб-интерфейс	7
2.3 Общее устройство веб-интерфейса	8
2.3.1 Элемент списка угроз	8
2.4 Поиск угроз	9
2.4.1 Подсказки по фильтрам	10
2.4.2 Быстрые фильтры и сортировка результатов	10
2.4.3 Операторы языка запросов	11
2.4.4 Перечень фильтров	12
2.5 Карточка угрозы	15
2.5.1 Шапка карточки	16
2.5.2 Вкладка «Подробности»	16
2.5.3 Вкладка «Затронутое ПО»	17
2.5.4 Вкладка «Эксплойты»	18
2.5.5 Вкладка «Шаблоны»	19
2.5.6 Вкладка «Упоминания»	19
2.5.7 Вкладка «CVSS и оценки»	20
2.5.8 Вкладка «Таймлайн»	21
2.5.9 Вкладка «Исследование»	21
2.6 Раздел «Вики»	22
2.7 Выгрузка результатов поиска	22
2.8 Создание и редактирование записей	23
2.9 Административный интерфейс	24
2.10 Горячие клавиши	25
3 Развёртывание экземпляра ПО	26
3.1 Общая информация	26

3.1.1	Состав стенда	26
3.1.2	Схема маршрутизации	27
3.1.3	Принципы развёртывания	27
3.2	Предварительные условия	27
3.2.1	Требования к узлу	27
3.2.2	Учётные данные и права доступа	28
3.2.3	Параметры окружения	28
3.2.4	Параметры административного интерфейса	29
3.3	Порядок развёртывания	30
3.3.1	Аутентификация в реестре контейнеров	30
3.3.2	Настройка параметров окружения	30
3.3.3	Развёртывание подсистемы данных	30
3.3.4	Развёртывание прикладной подсистемы	31
3.3.5	Приведение схемы базы данных к актуальной версии	31
3.4	Проверка работоспособности	32
3.5	Эксплуатация стенда	32
3.5.1	Обновление образов	32
3.5.2	Резервное копирование конфигурации	33
3.5.3	Остановка и удаление	33
4	Контакты технических специалистов для консультаций	34
5	Перечень сокращений и условных обозначений	35

1 ЦЕЛИ, НАЗНАЧЕНИЕ И ОБЛАСТИ ИСПОЛЬЗОВАНИЯ СИСТЕМЫ

Vulnum (далее — Система) представляет собой базу знаний об уязвимостях и угрозах информационной безопасности, объединяющую сведения из внешних источников и результаты собственных исследований.

Цели создания и области применения Системы:

- сбор и нормализация справочной информации об известных уязвимостях в различных видах программного обеспечения из внешних источников (NVD, cve.org, БДУ ФСТЭК России, GHSA, ZDI) и из собственных источников;
- сбор информации о способах эксплуатации уязвимостей — публичных и частных эксплойтов (Proof of Concept, далее — PoC), а также шаблонов проверки Nuclei;
- сбор информации об упоминании уязвимостей во внешних источниках и социальных сетях;
- расчёт метрик угрозы для каждой уязвимости — базовой оценки CVSS, вероятности эксплуатации EPSS, собственной оценки CybVSS, оценки RWDS, показателя распространённости и признака активной эксплуатации по каталогу CISA KEV.

Внедрение и использование Системы позволит обеспечить выполнение следующих задач:

- поиск, фильтрация и просмотр актуальных данных об уязвимостях, существующих в различных видах и версиях программного обеспечения;
- анализ активности упоминаний уязвимостей во внешних источниках и социальных сетях;
- оценка риска эксплуатации уязвимости в настоящее время;
- ведение собственных записей об уязвимостях и мисконфигурациях, их триаж и исследование;
- выгрузка результатов поиска для дальнейшей обработки во внешних системах.

Система предназначена для следующих ключевых пользователей:

- Администратор Системы — сотрудник оператора Системы, обладающий неограниченными полномочиями по действиям в Системе (добавление, блокировка и настройка пользователей Системы, настройка и запуск задач по сбору данных, настройка справочников);
- Оператор (исследователь) — пользователь, осуществляющий актуализацию сведений об уязвимостях, триаж поступающих записей и ведение задач исследования;
- Лицензированный пользователь — пользователь, обладающий лицензией и, в зависимости от типа лицензии, имеющий полномочия на просмотр данных по уязвимостям и способам их эксплуатации.

2 УДАЛЁННЫЙ ДОСТУП К ИНФРАСТРУКТУРЕ С РАЗВЁРНУТЫМ ЭКЗЕМПЛЯРОМ ПО

2.1 Доступ к узлу по протоколу SSH

Для администрирования стенда предоставляется доступ по протоколу SSH к узлу, на котором развёрнут экземпляр ПО.

Параметр	Значение
Адрес узла	51.250.30.38
Порт	22
Учётная запись администратора	root
Учётная запись оператора стенда	vulnum
Метод аутентификации	по ключу; аутентификация по паролю отключена

Приватный ключ для подключения пользователя root к узлу стенда:

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAABAG5vbmUAAAABbm9uZQAAAAAAAAABAAAAMwAAAAtz
c2gtZW
QyNTUxOQAAACAiSlGRcojyjcpgQ/JpW6IrVfKF597n74ofi+mI2mSR+AAAAKBiEI
QoYhCE
KAAAAAtzc2gtZWQyNTUxOQAAACAiSlGRcojyjcpgQ/JpW6IrVfKF597n74ofi+mI
2mSR+A
AAAEEDlkiEiyqpAOAkLzmTIVKkKFLlixUkv6Ogg2Xuo2NWNQCJKUZFyiPKNymBD8m
lboitV
8oXn3ufvih+L6YjaZJH4AAAAGnZ1bG51bUB2dWxudW0tdjMtc3RhZ2UtYWxsAQID
-----END OPENSSH PRIVATE KEY-----
```

Ключ сохраняется в файл, которому назначаются права доступа 600; при иных правах клиент SSH отклоняет использование ключа. Подключение выполняется командой:

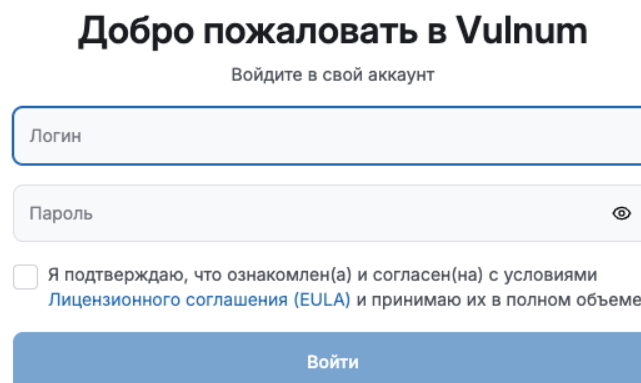
```
chmod 600 vulnum-stand-root
ssh -i vulnum-stand-root root@51.250.30.38
```

Учётная запись vulnum используется для повседневной эксплуатации стенда: в её домашнем каталоге размещается каталог ~/infra со сценариями развёртывания, и от её имени выполняются все команды раздела 3. Учётная запись обладает правом sudo без ввода пароля.

Внимание: параметры аутентификации в реестре контейнеров хранятся отдельно для каждой учётной записи. Команды загрузки образов выполняются от имени vulnum; при выполнении от имени root загрузка завершается ошибкой 401 Unauthorized.

2.2 Вход в веб-интерфейс

Необходимо перейти в веб-интерфейс по ссылке `https://vulnum.cbrdev.ru`.



Добро пожаловать в Vulnum

Войдите в свой аккаунт

Логин

Пароль

☐ Я подтверждаю, что ознакомлен(а) и согласен(на) с условиями [Лицензионного соглашения \(EULA\)](#) и принимаю их в полном объеме

Войти

Рисунок 1. Окно ввода логина и пароля

В поле «Логин» вводится имя учётной записи, в поле «Пароль» — пароль. Ввод чувствителен к регистру. Введённый пароль можно отобразить, нажав на пиктограмму в правой части поля.

Перед входом необходимо установить отметку подтверждения ознакомления с условиями Лицензионного соглашения (End User License Agreement, далее — EULA); полный текст соглашения открывается по ссылке «Лицензионного соглашения (EULA)». Кнопка «Войти» остаётся неактивной, пока не заполнены оба поля и не установлена отметка.

Учётные данные для доступа к демонстрационному стенду предоставляются отдельно; в настоящем документе они не приводятся. При необходимости их следует запросить у технических специалистов (раздел 4).

После успешного входа пользователю отображается главная страница веб-интерфейса — лента угроз.

2.3 Общее устройство веб-интерфейса

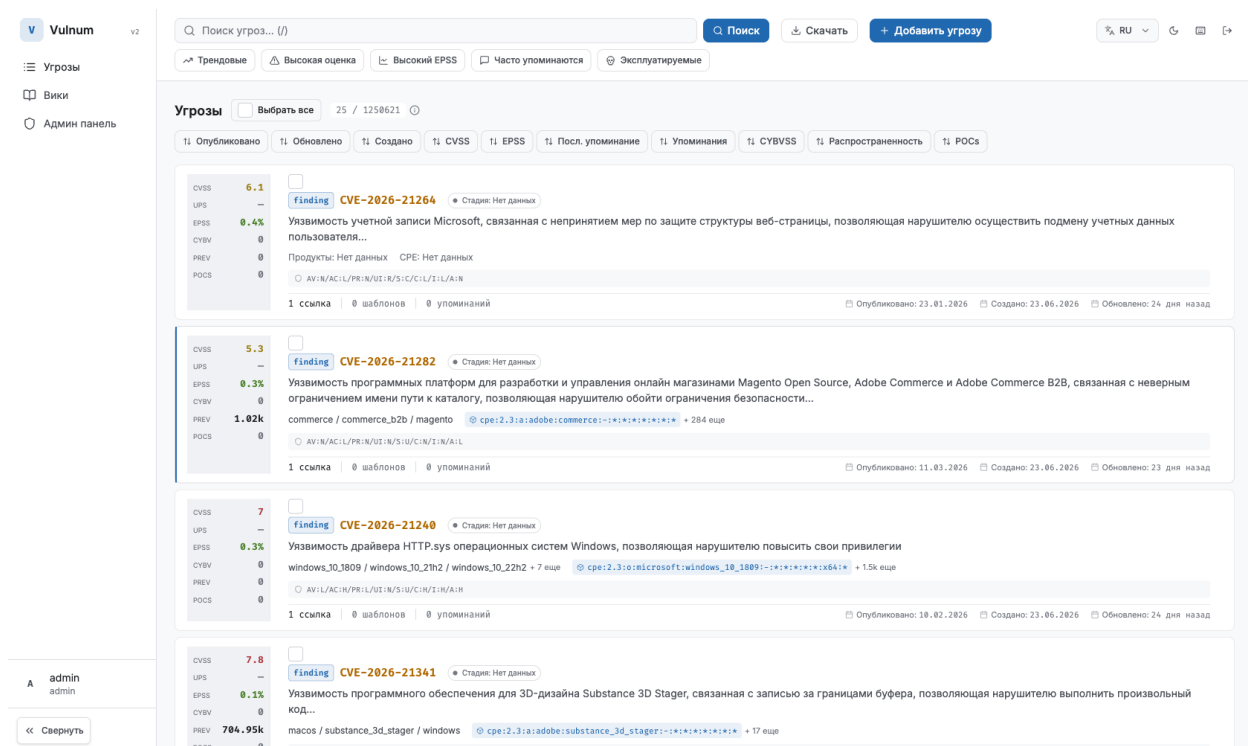


Рисунок 2. Главная страница веб-интерфейса (лента угроз)

Окно веб-интерфейса состоит из следующих областей:

- боковая панель навигации (слева) — разделы «Угрозы», «Вики» и «Админ панель», сведения о текущем пользователе и кнопка сворачивания панели;
- верхняя панель — строка поиска, кнопки «Поиск», «Скачать» и «Добавить угрозу», переключатель языка интерфейса (RU / EN), переключатель светлой и тёмной темы, справка по горячим клавишам и кнопка выхода из учётной записи;
- панель быстрых фильтров — «Трендовые», «Высокая оценка», «Высокий EPSS», «Часто упоминаются», «Эксплуатируемые»;
- рабочая область — список найденных записей с заголовком раздела, счётчиком результатов и панелью сортировок.

Счётчик результатов отображается в формате «показано / найдено». Постраничный просмотр ограничен первыми 10 000 записями: при большем числе совпадений выводится подсказка о необходимости уточнить запрос.

2.3.1 Элемент списка угроз

Каждая запись в списке содержит:

- панель числовых оценок слева — CVSS, UPS, EPSS, CYBV, PREV, POCS;
- представление (источник) записи — finding, nvd, cve.org, bdu, ghsa, zdi, cok; одна и та же уязвимость может присутствовать в ленте несколько раз — по одной записи на источник, плюс сводная карточка finding;

- идентификатор угрозы (CVE или идентификатор мисконфигурации) — ссылка на карточку угрозы;
- метки «KEV» (запись в каталоге CISA KEV), «PoC» (наличие эксплойта) и «Nuclei» (наличие шаблона);
- стадию триажа записи;
- заголовок и краткое описание уязвимости;
- перечень затронутых продуктов и строк CPE;
- строку вектора CVSS;
- счётчики ссылок-источников, шаблонов Nuclei и упоминаний;
- даты публикации в первоисточнике, добавления записи в Систему и последнего обновления записи;
- график активности упоминаний за период — для записей, по которым зафиксированы упоминания.

Числовые оценки в панели слева имеют следующее значение:

Обозначение	Расшифровка
CVSS	базовая оценка Common Vulnerability Scoring System по старшей доступной версии записи
UPS	оценка UPS; формируется по сигналам, отображаемым на вкладке «Таймлайн» карточки угрозы
EPSS	Exploit Prediction Scoring System — вероятность эксплуатации в ближайшие 30 дней (first.org)
CYBV	CybVSS — собственная оценка уязвимости Vulnum
PREV	оценка распространённости продукта или уязвимости (prevalence)
POCS	количество известных эксплойтов (PoC)

2.4 Поиск угроз

Поиск выполняется через строку поиска в верхней панели. Запрос вводится в формате «<фильтр> <оператор> <значение>» и подтверждается нажатием клавиши Enter либо кнопки «Поиск».

Допускается ввод текста без указания фильтра — в этом случае поиск выполняется по идентификатору и описаниям (на русском и английском языках) как поиск подстроки без учёта регистра. Такой поиск комбинируется с другими фильтрами, например: "buffer overflow" AND cvss.baseScore >= 9.

Значения фильтров, состоящие более чем из одного слова, необходимо заключать в кавычки. Несколько значений одного фильтра перечисляются через запятую, например `view = nvd, bdv`. Для составления сложных запросов применяются круглые скобки, например `(cvss.AV = N OR cvss.AV = A) AND kev = true`.

2.4.1 Подсказки по фильтрам

При нажатии на строку поиска отображается список доступных фильтров, сгруппированных по назначению, с примерами использования. Выбор подсказки подставляет фильтр в строку поиска.

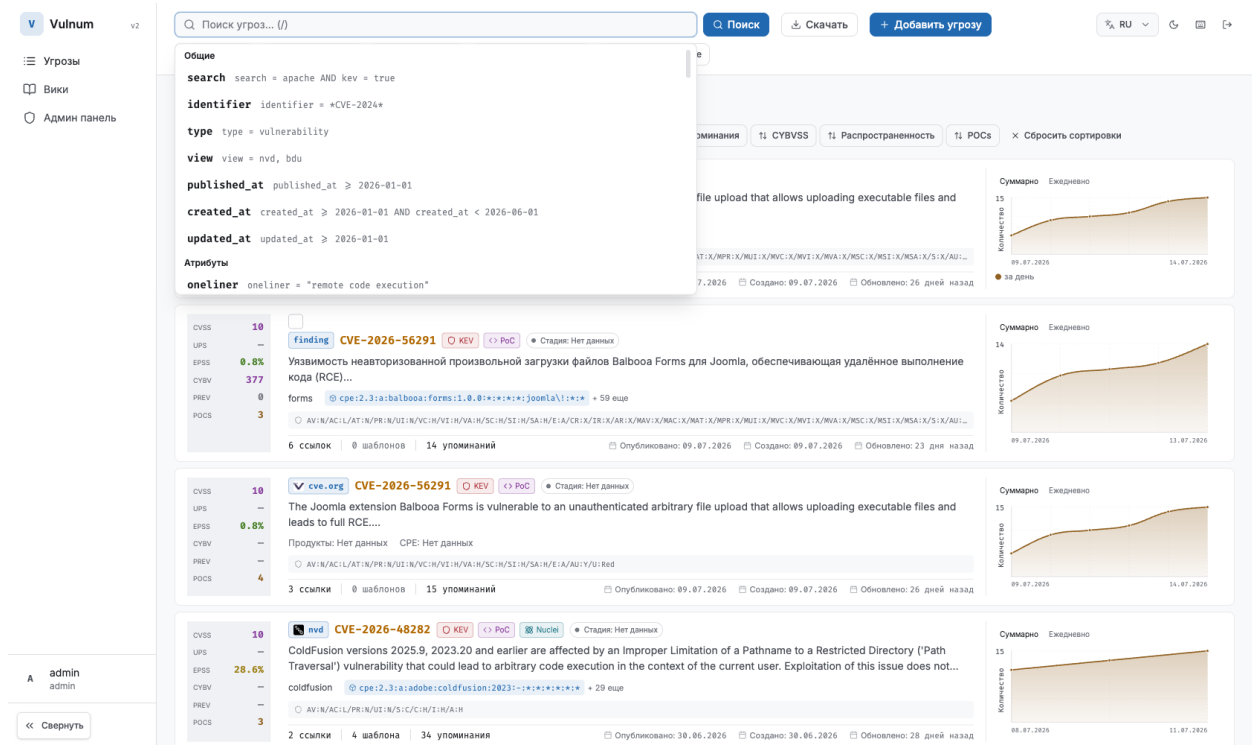


Рисунок 3. Список фильтров, доступный из строки поиска

2.4.2 Быстрые фильтры и сортировка результатов

Панель быстрых фильтров под строкой поиска позволяет применить типовой запрос одним нажатием. Например, фильтр «Эксплуатируемые» подставляет в строку поиска запрос `kev = true` — уязвимости из каталога активно эксплуатируемых CISA KEV.

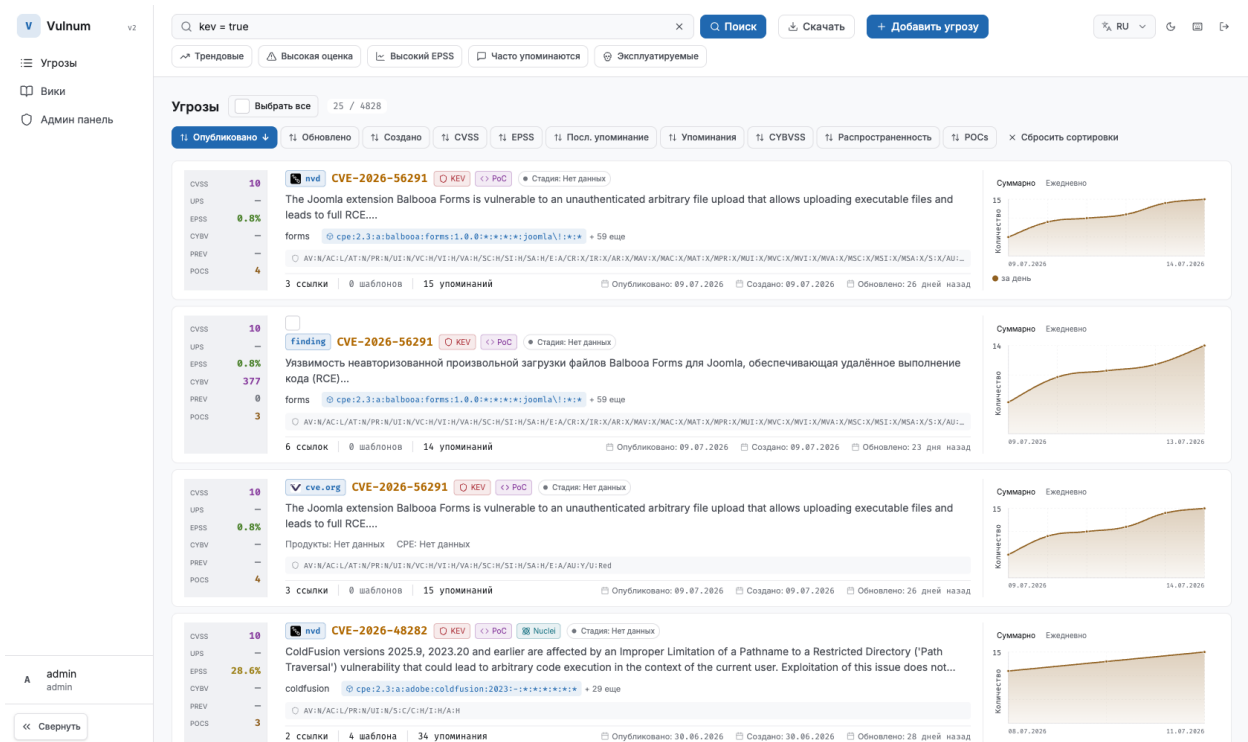


Рисунок 4. Результаты поиска по запросу `kev = true`

Результаты сортируются кнопками панели сортировок: «Опубликовано», «Обновлено», «Создано», «CVSS», «EPSS», «Посл. упоминание», «Упоминания», «CYBVSS», «Распространенность», «POCs». Повторное нажатие меняет направление сортировки; кнопка «Сбросить сортировки» возвращает порядок по умолчанию.

Отметка «Выбрать все» и отметки у отдельных записей позволяют выделить записи для групповых операций и последующей выгрузки.

2.4.3 Операторы языка запросов

Для сравнения значений используются следующие операторы:

Оператор	Описание	Пример
=	Равно. Применимо к строкам, числам, датам и булевым полям	<code>cvss.baseScore = 7</code>
==	Точное совпадение. Для <code>identifier</code> и <code>type</code> , где <code>=</code> работает как wildcard-поиск	<code>identifier == CVE-2024-1234</code>
!=	Не равно	<code>view != cok</code>
>	Больше (числовые и date-фильтры)	<code>pocs.count > 5</code>
>=	Больше или равно	<code>cvss.baseScore >= 7</code>
<	Меньше	<code>epss < 0.1</code>
<=	Меньше или равно	<code>nuclei.damage <= 0.5</code>

Для соединения условий используются логические операторы:

Оператор	Описание	Пример
AND	Нахождение записей, для которых выполняются сразу несколько условий	<code>cvss.AV = N AND cvss.PR = N</code>
OR	Нахождение записей, для которых выполняется хотя бы одно из условий	<code>cvss.AV = N OR cvss.AV = A</code>
NOT	Исключение записей из результатов поиска	<code>NOT kev = true</code>

2.4.4 Перечень фильтров

Общие фильтры

Фильтр	Описание	Пример
<code>search</code>	Поиск по идентификатору и описаниям (RU и EN) одновременно; вызывается автоматически при вводе значения без фильтра	<code>search = apache AND kev = true</code>
<code>identifier</code>	Поиск по идентификатору угрозы (CVE или Misconfig); * заменяет любые символы	<code>identifier = *CVE-2024*</code>
<code>type</code>	Тип записи: Vulnerability или Misconfiguration	<code>type = vulnerability</code>
<code>view</code>	Представление или источник записи: finding, cok, bdu, nvd, cve.org, ghsa, zdi	<code>view = nvd, bdu</code>
<code>published_at</code>	Дата публикации уязвимости в первоисточнике	<code>published_at >= 2026-01-01</code>
<code>created_at</code>	Дата добавления записи в базу знаний	<code>created_at >= 2026-01-01 AND created_at < 2026-06-01</code>
<code>updated_at</code>	Дата последнего обновления записи в базе знаний	<code>updated_at >= 2026-01-01</code>

Фильтры по оценкам

Фильтр	Описание	Пример
<code>epss.score</code>	Вероятность эксплуатации (EPSS) в ближайшие 30 дней, число от 0 до 1	<code>epss.score >= 0.5</code>
<code>epss.percentile</code>	Перцентиль EPSS относительно остальных уязвимостей	<code>epss.percentile >= 0.9</code>

kev	Наличие уязвимости в каталоге активно эксплуатируемых CISA KEV	kev = true
rwds	Оценка RWDS — оценка уязвимости по имеющимся о ней данным	rwds > 2
prevalence	Оценка распространённости продукта или уязвимости	prevalence > 100000
cybvss	CybVSS — собственная оценка уязвимости Vulnum	cybvss < 67.6
mentions	Наличие упоминаний	mentions = true
mentions.count	Количество упоминаний: всего либо за последний период вида «N by M days»	mentions.count > "5 by 7 days"

Фильтры по метрикам CVSS

Фильтр	Описание	Пример
cvss.baseScore	Базовый балл CVSS; по умолчанию — по старшей версии записи (v4 → v3.1 → v3 → v2)	cvss.baseScore >= 7
cvss.baseSeverity	Уровень severity: Low, Medium, High, Critical	cvss.baseSeverity = High
cvss.version	Версия CVSS (2, 3, 3.1, 4); дополнительно сужает остальные фильтры cvss.*	cvss.version = 3.1 AND cvss.baseScore >= 9
cvss.type	Тип оценки: Primary или Secondary	cvss.type = Primary
cvss.vector	Полная строка вектора CVSS	cvss.vector = "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H"
cvss.AV	Вектор атаки: N — сеть, A — смежная сеть, L — локальный, P — физический доступ	cvss.AV = N
cvss.AC	Сложность атаки: L — низкая, M — средняя (v2), H — высокая	cvss.AC = L
cvss.PR	Требуемые привилегии: N — не требуются, L — низкие, H — высокие	cvss.PR = N
cvss.UI	Взаимодействие с пользователем: N — не требуется, R — требуется	cvss.UI = N
cvss.S	Область воздействия: U — не меняется, C — меняется	cvss.S = C
cvss.C / cvss.I / cvss.A	Влияние на конфиденциальность, целостность и доступность: N — нет, L —	cvss.C = H

	низкое, Н — высокое; для v2 дополнительно P — частичное, C — полное	
cvss.Au	Аутентификация (CVSS v2): N — не требуется, S — однократная, M — многократная	cvss.Au = N

Фильтры по эксплойтам и шаблонам Nuclei

Фильтр	Описание	Пример
pocs	Наличие эксплойтов	pocs = true
pocs.count	Количество эксплойтов (PoC)	pocs.count > 5
pocs.verified	Наличие проверенных эксплойтов	pocs.verified = true
pocs.verified.count	Количество проверенных эксплойтов	pocs.verified.count >= 1
nuclei	Наличие шаблонов Nuclei	nuclei = true
nuclei.count	Количество шаблонов Nuclei	nuclei.count >= 1
nuclei.private	Наличие частных шаблонов Nuclei	nuclei.private = true
nuclei.private.count	Количество частных шаблонов Nuclei	nuclei.private.count > 0
nuclei.type	Тип шаблона: untyped, activecheck, safecheck, bannercheck-direct, bannercheck-indirect	nuclei.type = bannercheck-direct
nuclei.damage	Значение поля Damage в шаблонах Nuclei, число от 0 до 1	nuclei.damage < 0.5

Фильтры по затронутому программному обеспечению (CPE)

Фильтр	Описание	Пример
vendor	Быстрый поиск по вендору среди всех CPE записи	vendor = apache
product	Быстрый поиск по продукту среди всех CPE записи	product = httpd
cpe	Поиск по CPE-критерию записи, полная или частичная строка	cpe = cpe:2.3:o:microsoft:windows_server_2016:...
cpe.vendor	Поиск по вендору внутри конкретной CPE-записи	cpe.vendor = grafana

cpe.product	Поиск по продукту внутри конкретной CPE-записи	cpe.product = windows_7
cpe.productVersion	Поиск по версии продукта внутри конкретной CPE-записи	cpe.productVersion = 6.3.9600.20520

Фильтры по текстовым полям записи

Фильтры текстового поиска задаются с указанием языка (.ru либо .en): description, title, observation, remediation, reproduction_step, technical_detail, temporary_mitigation. Дополнительно доступны фильтры oneliner и curl_command, а также related.identifier — поиск по связанным идентификаторам. Пример: description.ru = "обход аутентификации".

Фильтры триажа

Фильтр	Описание	Пример
triage.status	Статус триажа: not viewed, viewed, wip, done, canceled, need_merge, merged	triage.status = wip
triage.updated	Дата последнего изменения статуса триажа	triage.updated >= 2026-05-01
triage.expert	Ответственный эксперт	triage.expert = "Igor Pervushin"
triage.milestone_id	Идентификатор этапа	triage.milestone_id = 180
triage.milestone_title	Точное название этапа	triage.milestone_title = E24.June.Release
triage.milestone_title_part	Часть названия этапа	triage.milestone_title_part = E24
triage.move_reason	Причина смены статуса	triage.move_reason = "security issue"

2.5 Карточка угрозы

При нажатии на идентификатор записи в списке осуществляется переход к карточке угрозы, содержащей полные сведения об уязвимости.

2.5.1 Шапка карточки

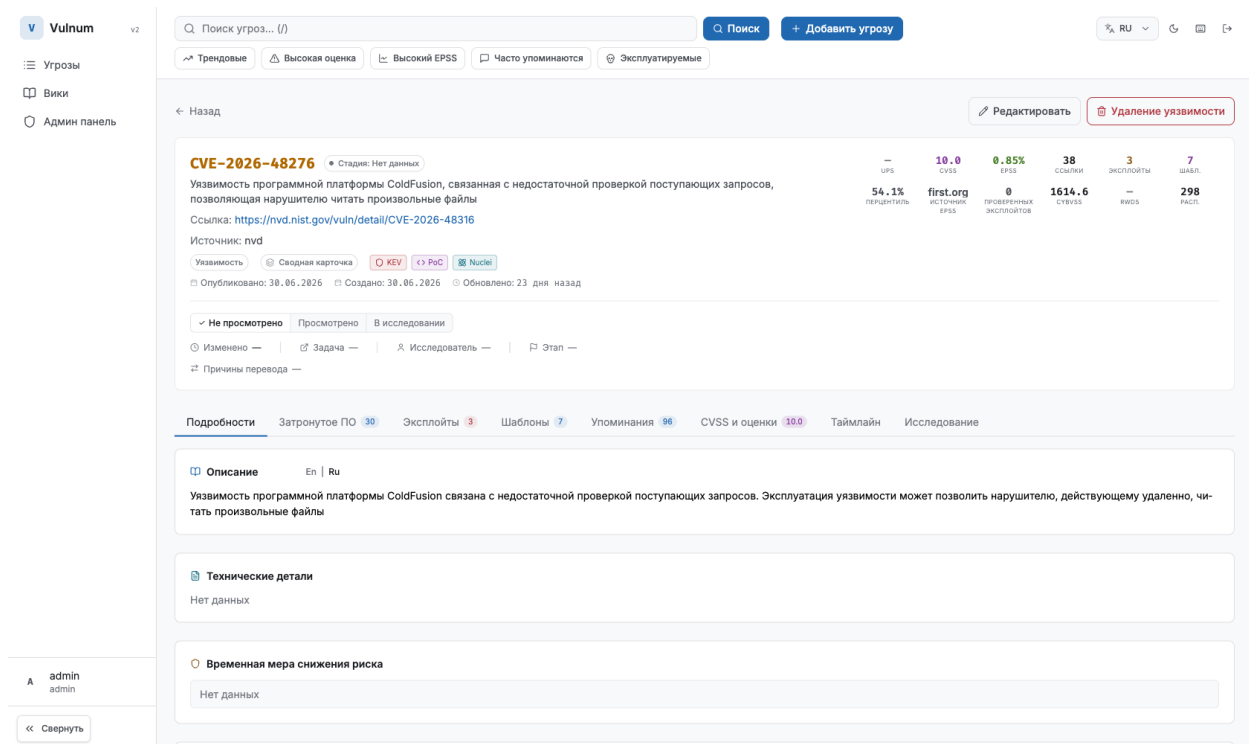


Рисунок 5. Карточка угрозы, вкладка «Подробности»

В верхней части карточки отображаются:

- идентификатор угрозы и стадия триажа;
- заголовок уязвимости, ссылка на первоисточник и наименование источника;
- метки типа записи («Уязвимость», «Сводная карточка») и признаков «KEY», «PoC», «Nuclei»;
- даты публикации, создания и обновления записи;
- панель оценок — UPS, CVSS, EPSS, число ссылок, эксплойтов и шаблонов, перцентиль EPSS, источник EPSS, число проверенных эксплойтов, SubVSS, RWDS и показатель распространённости;
- панель триажа — переключатель статуса («Не просмотрено», «Просмотрено», «В исследовании»), дата изменения, задача, ответственный исследователь, этап и причины перевода;
- кнопки «Редактировать» и «Удаление уязвимости» — доступны пользователям с соответствующими правами.

Ниже расположены вкладки: «Подробности», «Затронутое ПО», «Эксплойты», «Шаблоны», «Упоминания», «CVSS и оценки», «Таймлайн» и «Исследование». Рядом с названием вкладки указывается количество относящихся к ней записей.

2.5.2 Вкладка «Подробности»

Вкладка содержит следующие блоки:

- «Описание» — описание уязвимости с переключателем языка (En / Ru);
- «Технические детали» — технические сведения об уязвимости;
- «Временная мера снижения риска» — компенсирующие меры до установки исправления;
- «CWE» — перечень классов слабостей по классификации Common Weakness Enumeration с указанием источника;
- «Шаги по воспроизведению» — последовательность действий для воспроизведения уязвимости;
- «Шаги по исправлению» — рекомендации по устранению, включая ссылки на бюллетени производителя;
- «Oneliner» и «Curl-команда» — команды быстрой проверки наличия уязвимости;
- «Наблюдения» — результаты наблюдений по уязвимости;
- «Ссылки» — перечень ссылок-источников с указанием исходного источника, источника и тегов;
- «Связанные идентификаторы» — идентификаторы этой же уязвимости в других базах (например, БДУ ФСТЭК России), с переходом к соответствующим карточкам.

Блоки, по которым сведения отсутствуют, отображаются со значением «Нет данных».

2.5.3 Вкладка «Затронутое ПО»

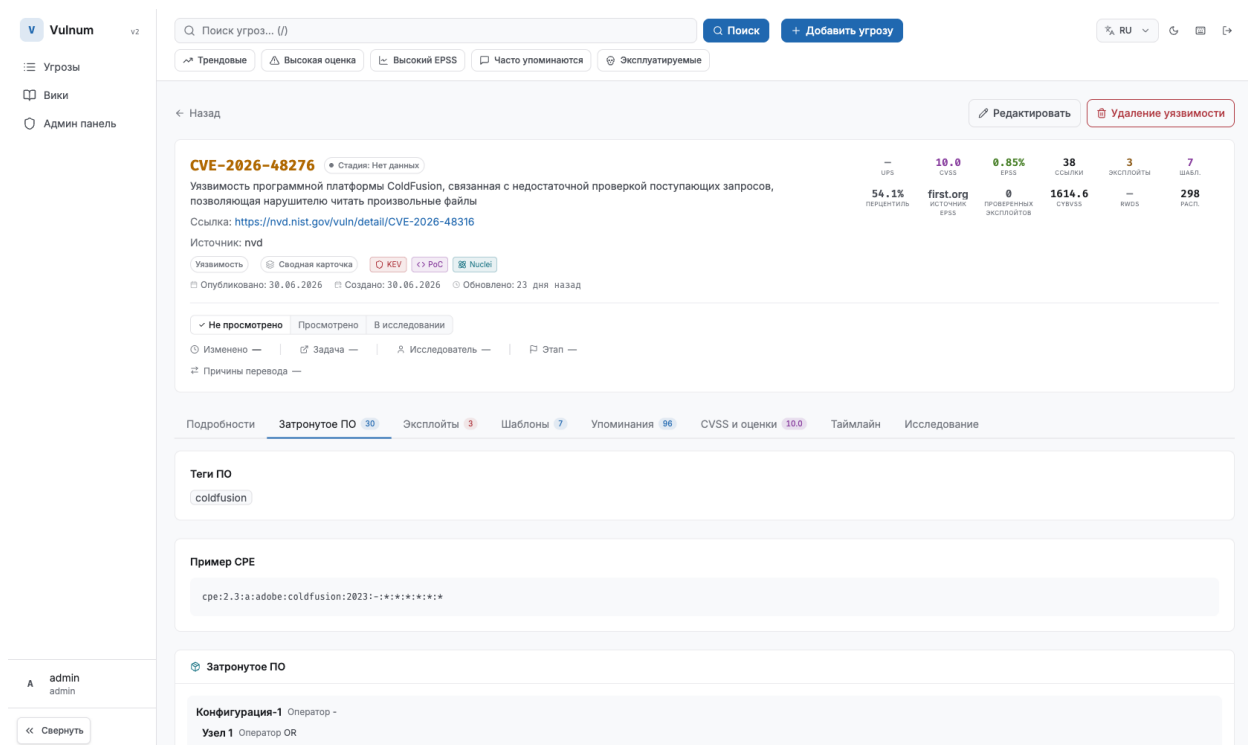


Рисунок 6. Карточка угрозы, вкладка «Затронутое ПО»

Вкладка содержит теги затронутого ПО, пример строки CPE и перечень CPE-конфигураций. Для каждой конфигурации приводятся операторы объединения

условий, а также таблица со столбцами «Уязвимый», «Критерий», «ID», «Версия от» и «До версии». Ссылка «Показать сопоставленные CPE» раскрывает перечень конкретных сопоставленных версий продукта.

2.5.4 Вкладка «Эксплойты»

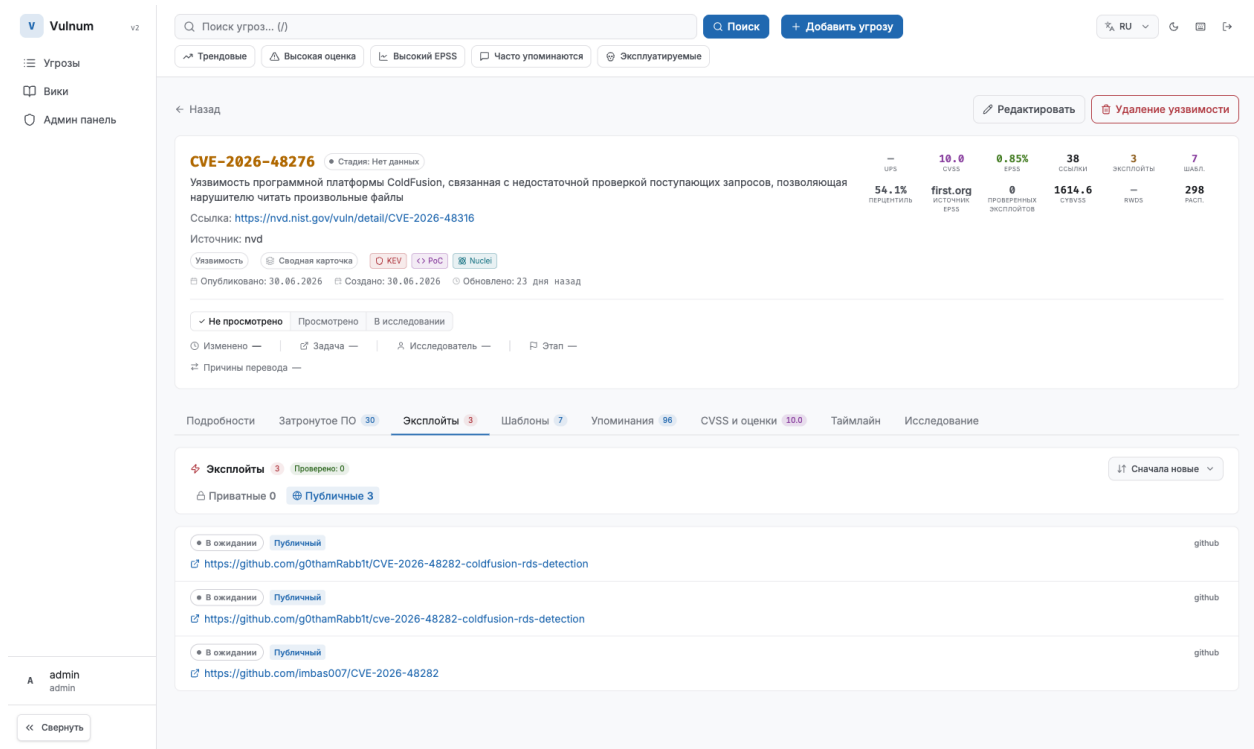


Рисунок 7. Карточка угрозы, вкладка «Эксплойты»

Вкладка содержит перечень известных эксплойтов (PoC) с указанием общего количества и числа проверенных. Записи разделены на приватные и публичные; предусмотрена сортировка по дате. Для каждого эксплойта отображаются статус проверки, признак публичности, источник и ссылка на код.

2.5.5 Вкладка «Шаблоны»

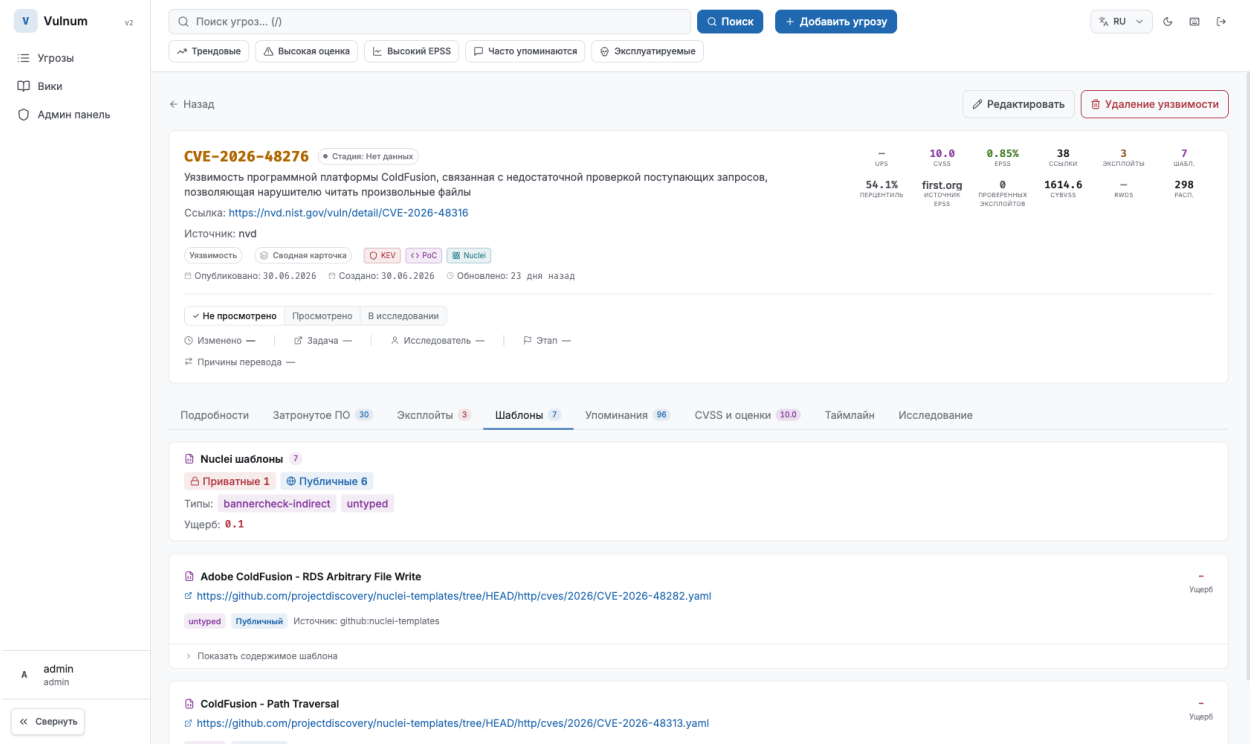


Рисунок 8. Карточка угрозы, вкладка «Шаблоны»

Вкладка содержит перечень шаблонов Nuclei для проверки наличия уязвимости с разделением на приватные и публичные, указанием типов шаблонов и значения Damage. Для каждого шаблона доступны наименование, ссылка, тип, источник, значение ущерба и кнопка «Показать содержимое шаблона».

2.5.6 Вкладка «Упоминания»

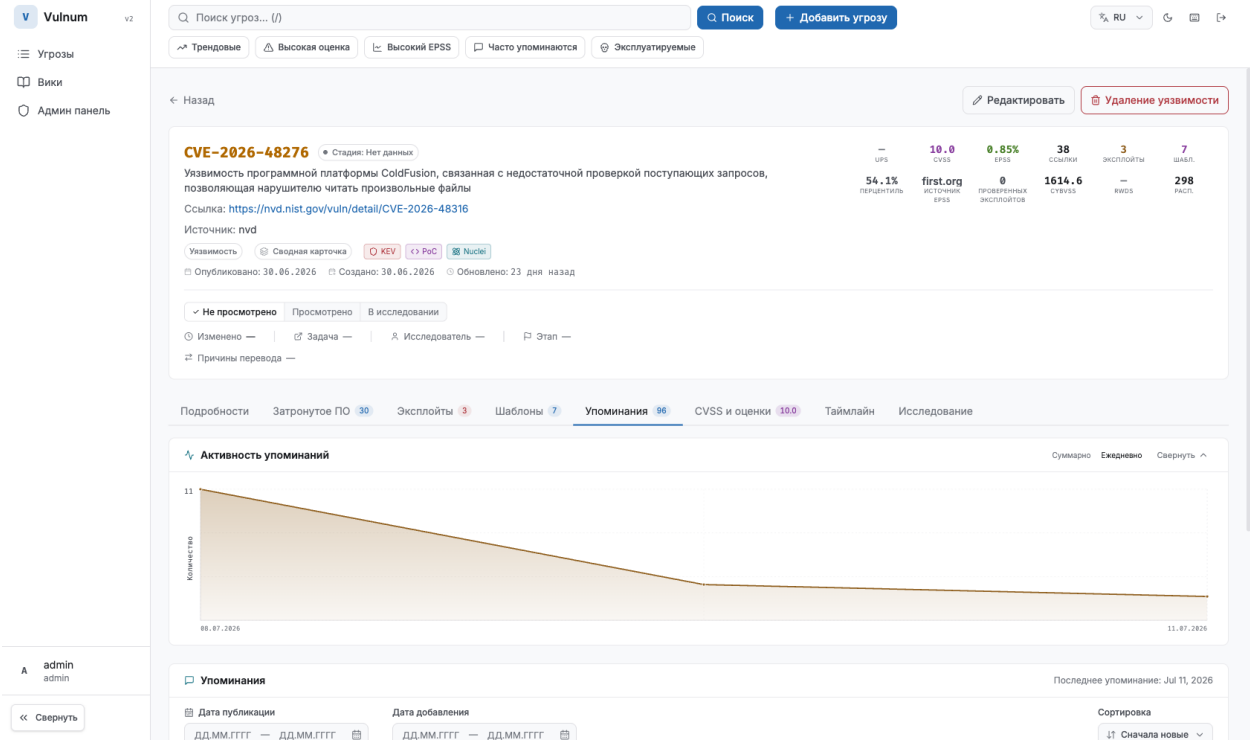


Рисунок 9. Карточка угрозы, вкладка «Упоминания»

Вкладка содержит график активности упоминаний с переключением режимов «Суммарно» и «Ежедневно», а также ленту упоминаний. Лента фильтруется по дате публикации и дате добавления и сортируется по дате. Для каждого упоминания отображаются источник (например, crowd, telegram), автор, текст сообщения, дата и ссылка «Перейти к источнику».

2.5.7 Вкладка «CVSS и оценки»

The screenshot displays the 'CVSS and ratings' tab for a specific vulnerability (CVE-2026-48276). The interface is divided into several sections:

- Header:** Includes a search bar, a 'Добавить угрозу' button, and a language selector (RU).
- Filters:** A row of buttons for 'Трендовые', 'Высокая оценка', 'Высокий EPSS', 'Часто упоминаются', and 'Эксплуатируемые'.
- Left Sidebar:** Contains navigation links for 'Vulnum', 'Угрозы', 'Вики', and 'Админ панель'.
- Main Content Area:**
 - Vulnerability Details:** CVE-2026-48276, description of the vulnerability, a link to the NVD entry, and the source (nvd).
 - CVSS Metrics:** A table showing scores for various metrics: CVSS (10.0), EPSS (0.85%), CPE (38), CWE (3), and others.
 - CVSS Breakdown:** A table titled 'Разбор вектора' showing the breakdown of the CVSS score into AV (Vector attack), AC (Attack complexity), and PR (Required privileges).
- Bottom Section:** A table titled 'CVSS 3.1 10.0 Critical' showing the CVSS score and severity.

Рисунок 10. Карточка угрозы, вкладка «CVSS и оценки»

Вкладка содержит оценки CVSS по всем доступным версиям (4.0, 3.1, 3.0, 2.0). Для каждой версии выводятся балл, уровень severity, тип оценки и источник, строка вектора, а также разбор вектора по метрикам: вектор атаки (AV), сложность атаки (AC), необходимые привилегии (PR), взаимодействие с пользователем (UI), область воздействия (S), влияние на конфиденциальность (C), целостность (I) и доступность (A). В блоке «Исходные метрики» приводятся источник, исходный источник, тип, версия, базовый балл, баллы эксплуатируемости и воздействия, временной и средовой баллы.

2.5.8 Вкладка «Таймлайн»

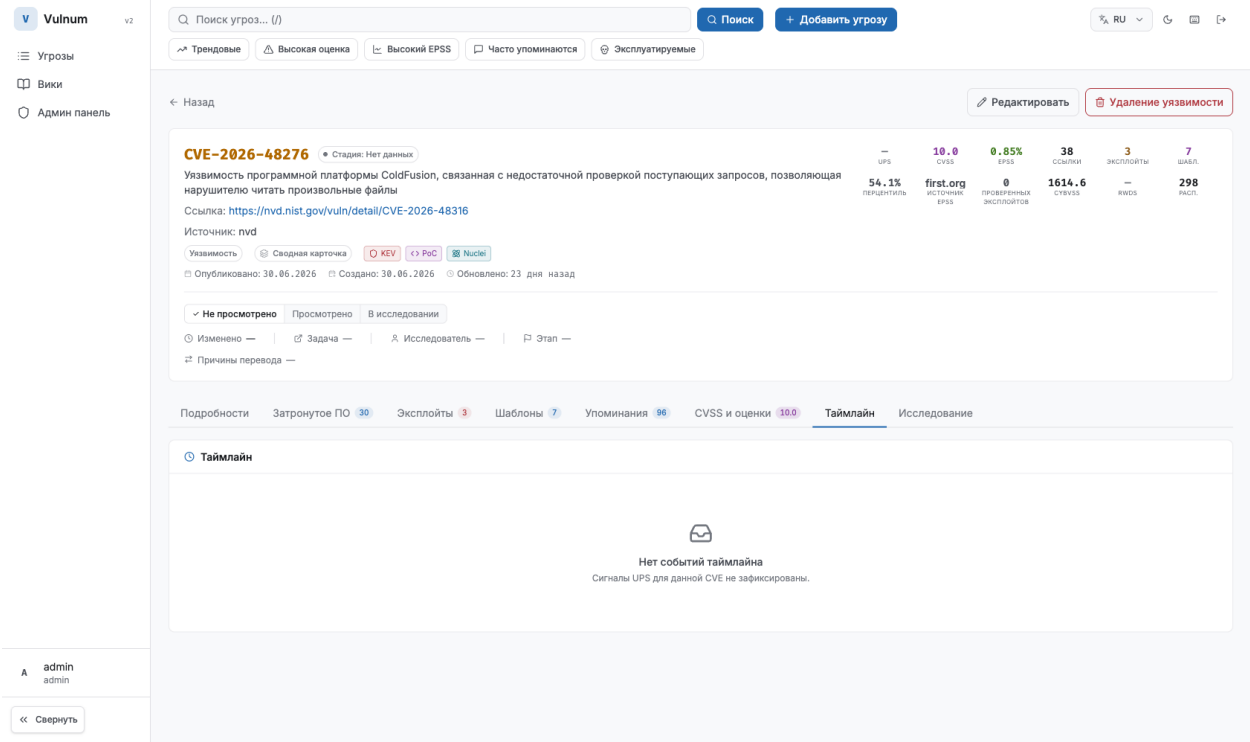


Рисунок 11. Карточка угрозы, вкладка «Таймлайн»

Вкладка отображает хронологию зафиксированных по уязвимости событий и сигналов UPS. При отсутствии событий выводится сообщение «Нет событий таймлайна».

2.5.9 Вкладка «Исследование»

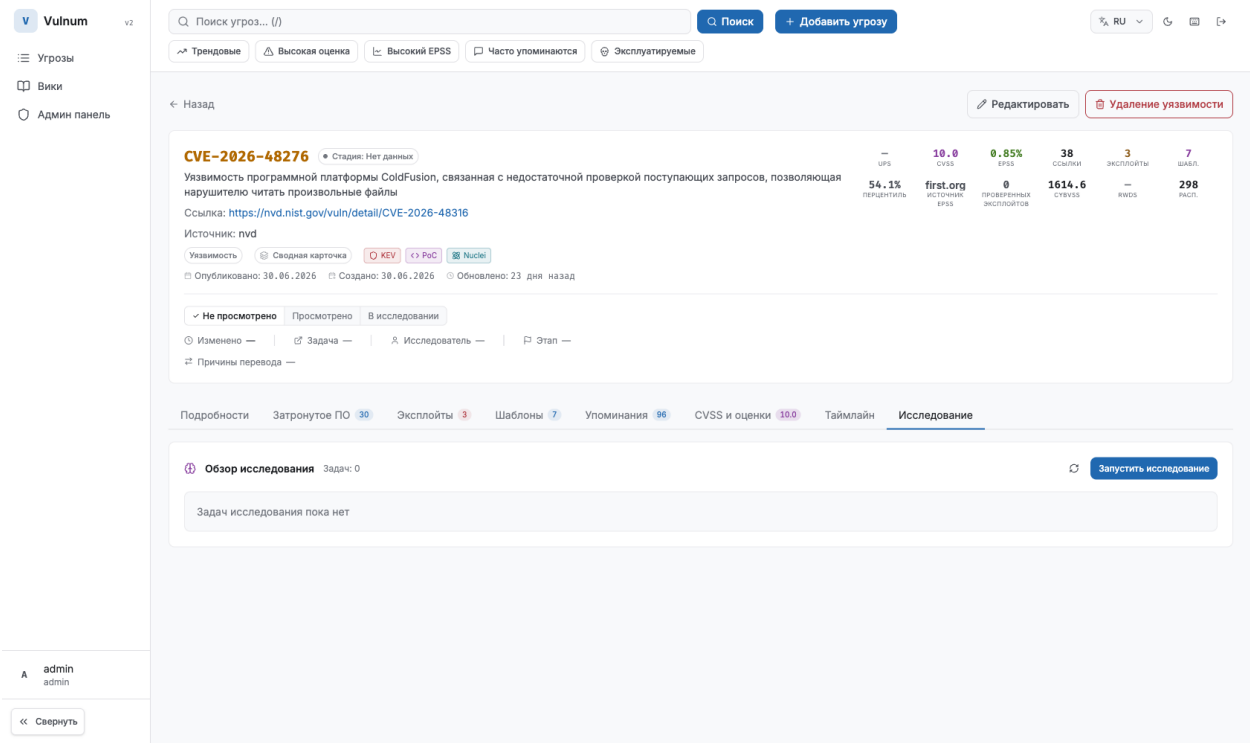


Рисунок 12. Карточка угрозы, вкладка «Исследование»

Вкладка содержит обзор задач исследования по уязвимости и счётчик задач. Кнопка «Запустить исследование» создаёт новую задачу исследования. При отсутствии задач выводится сообщение «Задач исследования пока нет».

2.6 Раздел «Вики»

The screenshot shows the 'Wiki' section of the Vulnum v2 interface. It contains a search bar at the top with a placeholder 'Поиск угроз... (/)' and buttons for 'Поиск' and 'Добавить угрозу'. Below the search bar are several filter buttons: 'Трендовые', 'Высокая оценка', 'Высокий EPSS', 'Часто упоминаются', and 'Эксплуатируемые'. The main content area is titled 'Составление запросов и фильтрация' and provides instructions on how to format search queries using filters, operators, and values. It includes examples of complex queries using parentheses and logical operators. Below this, there are two tables: 'Операторы сравнения' (Comparison Operators) and 'Логические операторы' (Logical Operators). The 'Операторы сравнения' table lists operators like '=', '==', '!=', '>', '≥', '<', and '≤' with their descriptions and examples. The 'Логические операторы' table lists 'AND' and 'OR' with their descriptions and examples.

Составление запросов и фильтрация

Чтобы сформировать запрос в строке поиска, введите фильтр, оператор и значение в формате: <фильтр> <оператор> <значение>. Список фильтров доступен при нажатии на строку поиска. Для составления сложных запросов можно использовать круглые скобки (): `cvss.AV = N OR cvss.AV = A` AND `kev = true`. Несколько значений одного фильтра перечисляются через запятую, например `view = nvd, bdu`. Можно ввести текст и без фильтра — поиск пойдёт по идентификатору и описаниям (RU и EN) как подстрока без учёта регистра; такой поиск комбинируется с другими фильтрами, например `"buffer overflow" AND cvss.baseScore ≥ 9`. **NB!** Значения для фильтров, состоящие более, чем из одного слова необходимо брать в кавычки.

Операторы сравнения

Оператор	Описание	Пример
=	Равно. Применимо к строкам, числам, датам и булевым полям	<code>cvss.baseScore = 7</code>
==	Точное совпадение. Для identifier и type, где = работает как wildcard-поиск	<code>identifier == CVE-2024-1234</code>
!=	Не равно	<code>view != cok</code>
>	Больше (числовые и date-фильтры)	<code>pocs.count > 5</code>
≥	Больше или равно	<code>cvss.baseScore ≥ 7</code>
<	Меньше	<code>epss < 0.1</code>
≤	Меньше или равно	<code>nuclei.damage ≤ 0.5</code>

Логические операторы

Для соединения фильтров используйте операторы

Оператор	Описание	Пример
AND	Используется для нахождения значений, у которых выполняются сразу несколько условий	<code>cvss.AV = N AND cvss.PR = H</code>
OR	Используется для нахождения значений, у которых выполняется хотя бы одно из заданных	<code>cvss.AV = N OR cvss.AV = A</code>

Рисунок 13. Раздел «Вики» — справка по составлению запросов

Раздел «Вики» содержит встроенную справку по языку запросов: правила составления запросов, таблицы операторов сравнения и логических операторов, а также полный перечень фильтров по группам с референтными значениями, описанием и примерами использования. Сведения из этого раздела приведены в подразделах 2.3.3 и 2.3.4 настоящего документа.

2.7 Выгрузка результатов поиска

Кнопка «Скачать» в верхней панели открывает окно «Выгрузка результатов поиска». Выгружаются записи, соответствующие текущему поисковому запросу.

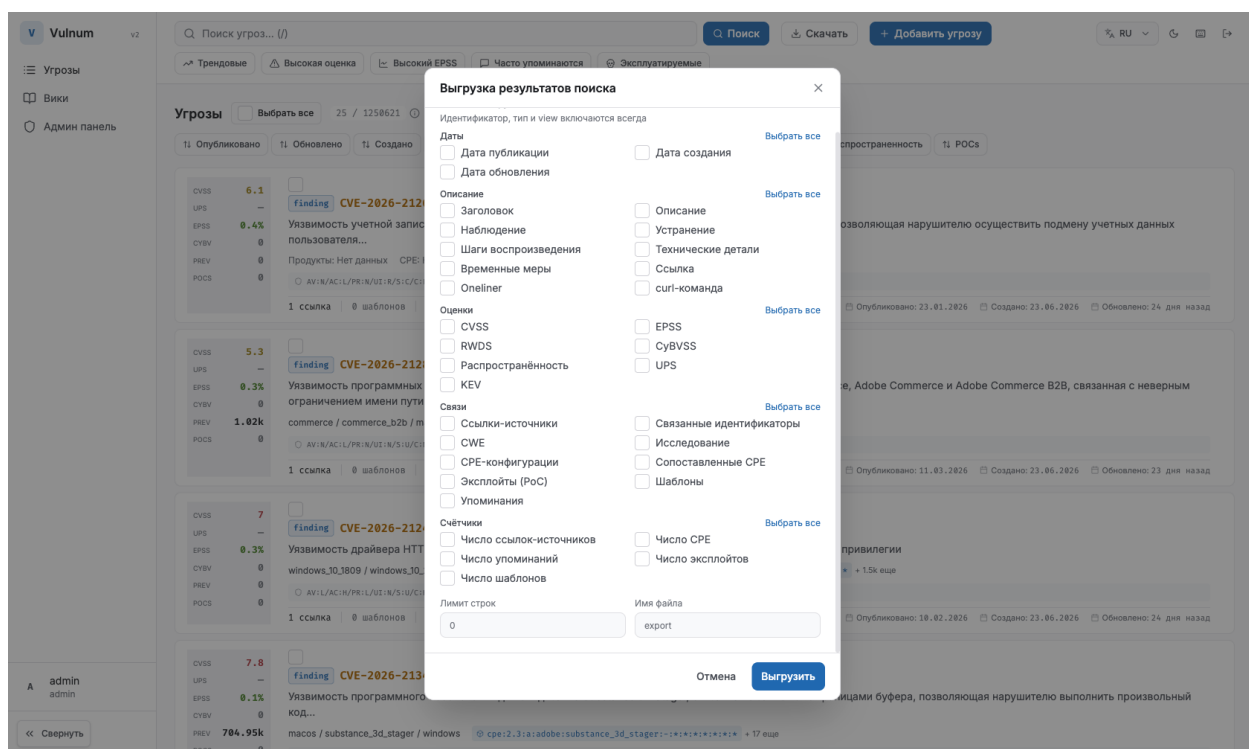


Рисунок 14. Окно выгрузки результатов поиска

Поля для выгрузки выбираются отметками и сгруппированы по разделам; идентификатор, тип и представление (view) включаются в выгрузку всегда. Для каждой группы доступна ссылка «Выбрать все».

- «Даты» — дата публикации, дата создания, дата обновления;
- «Описание» — заголовок, описание, наблюдение, устранение, шаги воспроизведения, технические детали, временные меры, ссылка, oneliner, curl-команда;
- «Оценки» — CVSS, EPSS, RWDS, CyBVSS, распространённость, UPS, KEV;
- «Связи» — ссылки-источники, связанные идентификаторы, CWE, исследование, CPE-конфигурации, сопоставленные CPE, эксплойты (PoC), шаблоны, упоминания;
- «Счётчики» — число ссылок-источников, число CPE, число упоминаний, число эксплойтов, число шаблонов.

В нижней части окна задаются лимит строк выгрузки и имя файла. Выгрузка запускается кнопкой «Выгрузить», отказ от выгрузки — кнопкой «Отмена».

2.8 Создание и редактирование записей

Кнопка «Добавить угрозу» в верхней панели открывает форму создания новой записи об уязвимости или мисконфигурации. Форма доступна пользователям с соответствующими правами.

The screenshot shows the 'Vulnum' web application interface. On the left is a sidebar with a 'Vulnum v2' header and three menu items: 'Угрозы' (Threats), 'Вики' (Wiki), and 'Админ панель' (Admin panel). The main content area at the top has a search bar 'Поиск угроз... (/)' and a '+ Добавить угрозу' button. Below the search bar are filter tabs: 'Трендовые', 'Высокая оценка', 'Высокий EPSS', 'Часто упоминаются', and 'Эксплуатируемые'. The main section is titled 'Все угрозы / Создание новой уязвимости' and contains a dropdown menu 'Создание новой уязвимости'. In the top right corner of the main area, there are language selectors 'RU' and 'EN', and a 'Создать' button. The form itself has several sections: 'Идентификатор' with a text input field; a tabbed interface with 'Подробности' (active), 'Эксплойты', 'Шаблоны', 'Упоминания', and 'CVSS и оценки'; 'Заголовок (RU)' with a text input field; 'Ссылка' with a text input field and a placeholder 'Введите ссылку в формате https://example.com'; and 'Описание' with a language selector 'RU', buttons for 'Редактирование' and 'Предпросмотр', a rich text editor toolbar, and a large text area for the description. At the bottom left, there is a user profile section showing 'A admin admin' and a '« Вернуть' button.

Рисунок 15. Форма создания новой уязвимости

В форме задаётся идентификатор записи, а содержимое распределено по вкладкам «Подробности», «Эксплойты», «Шаблоны», «Упоминания» и «CVSS и оценки». Переключатель RU / EN задаёт язык заполняемых текстовых полей.

Текстовые блоки («Описание», «Технические детали», «Временная мера снижения риска», «Шаги по воспроизведению», «Шаги по исправлению», «Наблюдения») заполняются в редакторе с разметкой и режимом предпросмотра. Дополнительно заполняются заголовок, ссылка, поля «Oneliner» и «Curl-команда» (до 8 000 символов каждое), перечни CWE, ссылок и связанных идентификаторов.

Запись сохраняется кнопкой «Создать». Редактирование существующей записи выполняется кнопкой «Редактировать» в карточке угрозы, удаление — кнопкой «Удаление уязвимости».

2.9 Административный интерфейс

Административный интерфейс развёрнут как отдельный компонент и доступен по адресу <https://vulnum.cbrdev.ru/admin/>. Переход выполняется также по ссылке «Админ панель» в боковой панели навигации основного веб-интерфейса.

Интерфейс предоставляет доступ к разделам статистики использования, справочнику причин перевода записей между статусами триажа, настройке фильтров уведомлений и правилам пороговых значений истории.

Вход выполняется через собственную форму `/admin/sign-in`. Учётные данные администратора задаются на этапе сборки образа; сессия сохраняется в локальном хранилище браузера.

Внимание: учётные данные административного интерфейса не задаются в файле параметров окружения. Их изменение выполняется пересборкой образа (подраздел 3.2.4).

2.10 Горячие клавиши

Перечень горячих клавиш открывается кнопкой в верхней панели либо нажатием клавиши «?».

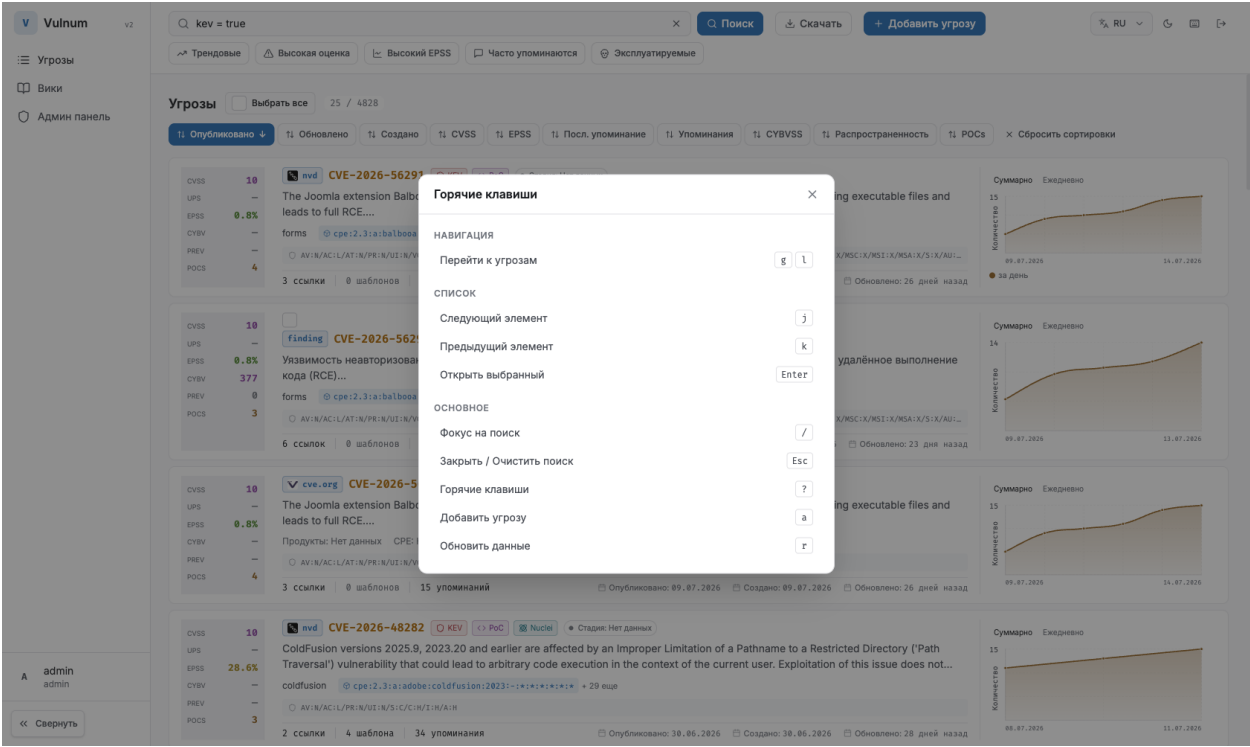


Рисунок 16. Окно «Горячие клавиши»

Клавиша	Действие
g, l	Перейти к угрозам
j	Следующий элемент списка
k	Предыдущий элемент списка
Enter	Открыть выбранный элемент
/	Фокус на строку поиска
Esc	Заккрыть окно или очистить поиск
?	Показать перечень горячих клавиш
a	Добавить угрозу
r	Обновить данные

3 РАЗВЁРТЫВАНИЕ ЭКЗЕМПЛЯРА ПО

Настоящий раздел описывает порядок развёртывания автономного стенда базы знаний по уязвимостям Vulnum (далее — стенд), состав используемых учётных данных и требования к их области действия. Раздел предназначен для инженеров, выполняющих установку и эксплуатацию стенда.

3.1 Общая информация

3.1.1 Состав стенда

Стенд представляет собой набор контейнеризованных компонентов, развёртываемых на одном узле. Компоненты разделены на две подсистемы, каждой из которых соответствует отдельный проект Docker Compose.

Подсистема данных и прокси-сервера — проект `setup`:

- обратный прокси-сервер Caddy — единая точка входа, терминирование протокола Transport Layer Security (далее — TLS) и маршрутизация запросов;
- система управления базами данных (далее — СУБД) PostgreSQL — хранение данных базы знаний;
- поисковый механизм Elasticsearch — индексы поиска;
- объектное хранилище MinIO — хранение файлов выгрузок и содержимого PoC;
- служебная задача minio-init — однократное создание разделов (bucket) объектного хранилища; завершается после выполнения.

Прикладная подсистема — проект `vulnum`:

- прикладной программный интерфейс (Application Programming Interface, далее — API) базы знаний — компонент `api`;
- пользовательский интерфейс (User Interface, далее — UI) — компонент `ui`;
- административный интерфейс — компонент `admin`, обслуживает раздел `/admin`;
- обработчик фоновых задач — компонент `worker`; выполняет построение агрегатов, ведение журнала, индексацию PoC и формирование файлов выгрузок;
- загрузчик внешних источников — компонент `downloader`; на автономном стенде все источники отключены.

Внимание: компонент `worker` обязателен к развёртыванию. Обработка очередей отложенных операций выполняется именно им; при отсутствии компонента очереди накапливаются, а агрегированные показатели и выгрузки не формируются.

Управление осуществляется двумя проектами системы Docker Compose: `setup` (подсистема данных и прокси-сервер) и `vulnum` (прикладная подсистема), запускаемыми через сценарий-обёртку `docker/dc`.

3.1.2 Схема маршрутизации

Внешние запросы принимает прокси-сервер Caddy и распределяет их между компонентами:

Путь запроса	Компонент	Назначение
<code>/api/kb/*</code>	<code>api</code>	программный интерфейс базы знаний
<code>/admin/*</code>	<code>admin</code>	административный интерфейс
<code>/api/login*</code> , <code>/api/logout*</code>	<code>ui</code>	обработка входа и выхода
остальные пути	<code>ui</code>	основной веб-интерфейс

3.1.3 Принципы развёртывания

При развёртывании стенда соблюдаются следующие принципы:

— **Восстановление из резервных копий.** База данных и поисковые индексы восстанавливаются из заранее подготовленных резервных копий (`kb_db.dump`, каталог `elastic_dump`). Резервная копия базы данных содержит структуру и данные; при необходимости приведения схемы к актуальной версии применяются миграции (подраздел 3.3.5).

— **Минимизация прав.** Для загрузки образов используется отдельный сервисный аккаунт (далее — СА) с правом только на чтение и только на два целевых репозитория. Иные ресурсы облачной платформы для стенда недоступны.

— **Локальность секретов.** Все прочие учётные данные (пароли СУБД и объектного хранилища, учётные записи UI) задаются локально в файле параметров окружения и за пределы стенда не передаются.

— **Неизменяемость образов.** Каждый образ публикуется под тегом, содержащим идентификатор исходного коммита. Тег не переиспользуется, что обеспечивает воспроизводимость состава стенда и однозначность отката.

3.2 Предварительные условия

3.2.1 Требования к узлу

На узле развёртывания должны быть установлены:

- Docker с подсистемой Docker Compose (версия 2 и выше);
- сетевой доступ к реестру контейнеров `cr.yandex`;
- каталог `~/infra`, содержащий сценарии развёртывания (`docker/dc`, `docker/functions`, `docker/prepare`) и резервные копии.

3.2.2 Учётные данные и права доступа

Единственным внешним токеном стенда является ключ СА для загрузки образов из реестра контейнеров.

Область действия ключа ограничена репозиториями компонентов стенда с правом только на чтение:

Репозиторий	Компонент
.../cok/vulnum/rooster-knowledge-base/api	api
.../cok/vulnum/rooster-knowledge-base/worker	worker
.../cok/vulnum/rooster-knowledge-base/downloader	downloader
.../cok/vulnum/rooster-knowledge-base/migrator	служебный образ миграций
.../cok/vulnum/knowledgebase-ui	ui
.../cok/vulnum/vulnum-admin-ui	admin

Полный префикс репозитория — `cr.yandex/crpop4bvjfl6mk2a7233`. Роль сервисного аккаунта — `container-registry.images.puller`; она назначается отдельно для каждого репозитория.

Файл ключа `kb-stand-puller-key.json` размещается на узле стенда с правами доступа `600` и не подлежит помещению в систему контроля версий.

Внимание: при добавлении в состав стенда нового компонента соответствующий репозиторий создаётся при первой публикации образа и прав доступа не наследует. До назначения роли загрузка образа завершается ошибкой `403 Forbidden`.

3.2.3 Параметры окружения

Параметры задаются в файле `~/infra/.env`:

Параметр	Назначение
PROXY_NETWORK	имя сети Docker для связи прокси-сервера с компонентами <code>api</code> и <code>ui</code>
SHARED_NETWORK	имя сети Docker для связи <code>api</code> с СУБД и поисковым механизмом
POSTGRES_USER, POSTGRES_PASSWORD, POSTGRES_DB	учётные данные и имя базы данных; должны соответствовать резервной копии
DOMAIN	адрес стенда (IP-адрес либо имя узла)
AUTH_USER, AUTH_PASSWORD	учётная запись пользователя UI
AUTH_ADMIN_USER, AUTH_ADMIN_PASSWORD	учётная запись администратора UI

IP_DOMAIN_SELF_SIGNED	адрес, для которого выпускается самоподписанный сертификат TLS
MINIO_ROOT_USER, MINIO_ROOT_PASSWORD	учётные данные объектного хранилища
S3_EXPORT_BUCKET	имя раздела объектного хранилища для файлов выгрузок
S3_POC_BUCKET	имя раздела объектного хранилища для содержимого PoC

Пример содержимого файла:

```

PROXY_NETWORK=proxy
SHARED_NETWORK=shared

# postgres
POSTGRES_USER=kb_user
POSTGRES_PASSWORD=<пароль>
POSTGRES_DB=kb_db

DOMAIN=<IP-адрес или имя узла>

AUTH_USER=user
AUTH_PASSWORD=<пароль>
AUTH_ADMIN_USER=admin
AUTH_ADMIN_PASSWORD=<пароль>

# minio
MINIO_ROOT_USER=vulnum
MINIO_ROOT_PASSWORD=<пароль>
S3_EXPORT_BUCKET=exports
S3_POC_BUCKET=pocs

```

3.2.4 Параметры административного интерфейса

Административный интерфейс представляет собой статическое веб-приложение. Его параметры считываются на этапе сборки образа и включаются в состав опубликованных файлов; в файле параметров окружения они не задаются и в среде выполнения контейнера не действуют.

Параметр сборки	Назначение
VITE_DEPLOY_TARGET	базовый адрес программного интерфейса; для стенда — /api
VITE_KB_PROXY_SERVICE	сегмент маршрута программного интерфейса; для стенда — kb

VITE_AUTH_ADMIN_USER, VITE_AUTH_ADMIN_PASSWORD	учётная запись администратора
VITE_AUTH_USER, VITE_AUTH_PASSWORD	учётная запись пользователя; в административный интерфейс не допускается

Внимание: изменение учётных данных административного интерфейса выполняется пересборкой и повторной публикацией образа с последующим обновлением тега в конфигурации стенда.

3.3 Порядок развёртывания

3.3.1 Аутентификация в реестре контейнеров

```
cat kb-stand-puller-key.json \
  | docker login --username json_key \
    --password-stdin cr.yandex
```

Признак успешного выполнения — сообщение `Login Succeeded`. Использование ключа СА в качестве пароля не имеет срока действия; параметры аутентификации сохраняются до отзыва ключа.

Внимание: параметры аутентификации сохраняются в домашнем каталоге учётной записи, от имени которой выполнена команда. Все последующие команды загрузки образов выполняются от имени той же учётной записи.

3.3.2 Настройка параметров окружения

```
cd infra
```

В файле `.env` указывается адрес стенда — параметр `DOMAIN`. Прочие параметры при первичной установке приводятся в соответствие с подразделом 3.2.3.

При первичном развёртывании на узле дополнительно создаются сети Docker (выполняется однократно; при наличии сетей шаг пропускается):

```
set -a; . ./env; set +a
bash docker/prepare
```

3.3.3 Развёртывание подсистемы данных

```
docker/dc setup up -d
```

Команда развёртывает СУБД PostgreSQL, поисковый механизм Elasticsearch, объектное хранилище MinIO и прокси-сервер Caddy, после чего выполняется автоматическое восстановление базы данных и поисковых индексов из резервных копий и создание разделов объектного хранилища.

Внимание: восстановление занимает от 20 до 30 минут. До его завершения прикладная подсистема не развёртывается.

Контроль готовности:

```
# состояние компонентов (healthy)
docker/dc setup ps

# признак завершения — сообщение "restore done"
docker/dc setup logs -f elastic-restore

# признак создания разделов — сообщение "buckets ready"
docker/dc setup logs minio-init
```

3.3.4 Развёртывание прикладной подсистемы

По завершении восстановления:

```
docker/dc vulnum up -d
```

Команда развёртывает компоненты api, ui, admin, worker и downloader. После запуска стенд доступен по адресу <https://<DOMAIN>>, административный интерфейс — по адресу <https://<DOMAIN>/admin/>.

Используется самоподписанный сертификат TLS, в связи с чем браузер выводит предупреждение о недоверенном сертификате; предупреждение подтверждается оператором. Вход в UI выполняется под учётной записью, заданной параметрами AUTH_USER либо AUTH_ADMIN_USER (порядок входа приведён в подразделе 2.1).

3.3.5 Приведение схемы базы данных к актуальной версии

Шаг выполняется, если версия схемы в восстановленной резервной копии ниже версии, требуемой образами компонентов. Текущая версия схемы определяется командой:

```
docker exec setup-postgres-1 psql -U kb_user -d kb_db -tAc \
    "SELECT version, dirty FROM schema_migrations;"
```

Значение dirty = f означает корректно завершённое применение миграций. При несовпадении версий миграции применяются служебным образом migrator.

Внимание: восстановление резервной копии выполняется без остановки при ошибках. По завершении шага 3.3.3 рекомендуется убедиться в полноте восстановления — сверить количество записей в основных таблицах с ожидаемым.

3.4 Проверка работоспособности

```
# состояние компонентов
docker/dc vulnum ps

# доступность API (служебный порт)
docker/dc vulnum exec api \
    wget -qO- http://localhost:8081/healthz

# возврат данных API (прикладной порт)
docker/dc vulnum exec api \
    wget -qO- 'http://localhost:8080/v1/cwes' \
    | head -c 300

# сквозная проверка через прокси-сервер
curl -sk 'https://<DOMAIN>/api/kb/v1/cwes' \
    | head -c 300

# сквозная проверка основного веб-интерфейса
curl -skI 'https://<DOMAIN>/'

# сквозная проверка административного интерфейса
curl -skI 'https://<DOMAIN>/admin/'
```

Признаки корректной работы:

- все компоненты в состоянии healthy;
- возврат данных в формате JavaScript Object Notation (далее — JSON) и отображение перечня записей в UI;
- код ответа 307 с перенаправлением на страницу входа для основного веб-интерфейса и 200 для административного;
- отсутствие сообщений уровня FATAL в журналах компонентов api и worker.

3.5 Эксплуатация стенда

3.5.1 Обновление образов

Образы публикуются под неизменяемыми тегами, содержащими идентификатор исходного коммита. Обновление выполняется указанием нового

тега в файле `docker/vulnum/docker-compose.yml` с последующей загрузкой и перезапуском:

```
docker/dc vulnum pull
docker/dc vulnum up -d --remove-orphans
```

Откат к предыдущей версии выполняется возвратом прежнего значения тега и повторным выполнением тех же команд. Принудительное пересоздание контейнеров (`--force-recreate`) не требуется: изменение тега само по себе приводит к пересозданию.

3.5.2 Резервное копирование конфигурации

Перед изменением файлов конфигурации создаётся их резервная копия:

```
cd ~/infra
TS=$(date +%F-%H%M)
cp -a .env .env.bak-$TS
cp -a docker/setup/docker-compose.yml docker/setup/docker-
compose.yml.bak-$TS
cp -a docker/vulnum/docker-compose.yml docker/vulnum/docker-
compose.yml.bak-$TS
```

3.5.3 Остановка и удаление

```
# остановка прикладной подсистемы
docker/dc vulnum down

# остановка подсистемы данных, тома с данными сохраняются
docker/dc setup down

# остановка с удалением томов
docker/dc setup down -v
```

Внимание: выполнение `docker/dc setup down -v` удаляет данные, включая содержимое объектного хранилища. Последующий запуск повлечёт полное восстановление из резервных копий продолжительностью 20–30 минут.

4 КОНТАКТЫ ТЕХНИЧЕСКИХ СПЕЦИАЛИСТОВ ДЛЯ КОНСУЛЬТАЦИЙ

Контакты технических специалистов, которые смогут проконсультировать по процессу развёртывания и настройки экземпляра ПО и его функционирования:

Максим Коваль-Навроцкий:

- контактный телефон: +7 (926) 363-29-79;
- контактный адрес электронной почты: mkn@cyberok.ru.

5 ПЕРЕЧЕНЬ СОКРАЩЕНИЙ И УСЛОВНЫХ ОБОЗНАЧЕНИЙ

Сокращение	Расшифровка
API	Application Programming Interface — программный интерфейс приложения
CPE	Common Platform Enumeration — унифицированное обозначение программной платформы
CVE	Common Vulnerabilities and Exposures — идентификатор известной уязвимости
CVSS	Common Vulnerability Scoring System — система оценки критичности уязвимостей
CWE	Common Weakness Enumeration — классификация недостатков программного обеспечения
CybVSS	собственная оценка критичности уязвимости, рассчитываемая Системой
EPSS	Exploit Prediction Scoring System — оценка вероятности эксплуатации уязвимости
EULA	End User License Agreement — лицензионное соглашение с конечным пользователем
IAM	Identity and Access Management — управление идентификацией и доступом
JSON	JavaScript Object Notation — текстовый формат обмена данными
KEV	Known Exploited Vulnerabilities — каталог активно эксплуатируемых уязвимостей CISA
PoC	Proof of Concept — эксплойт, подтверждающий возможность эксплуатации уязвимости
RWDS	оценка уязвимости, формируемая по имеющимся о ней данным
S3	протокол доступа к объектному хранилищу
TLS	Transport Layer Security — протокол защиты транспортного уровня
SSH	Secure Shell — протокол защищённого удалённого доступа
UI	User Interface — пользовательский интерфейс
UPS	оценка, формируемая по сигналам, отображаемым на вкладке «Таймлайн»
CA	сервисный аккаунт — учётная запись для программного доступа
СУБД	система управления базами данных