

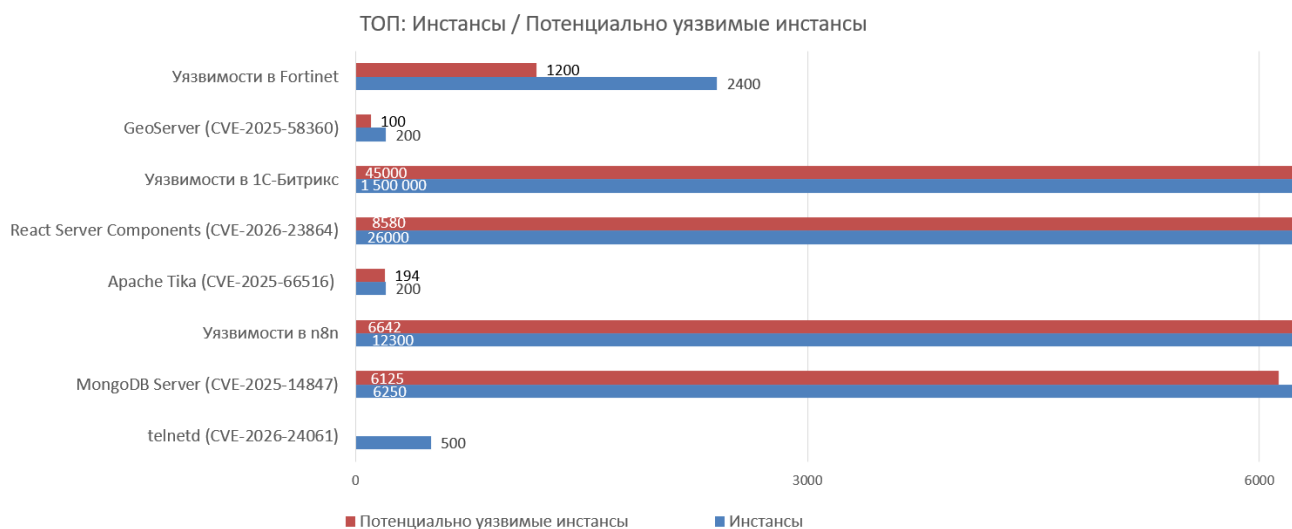
Левиафаны Рунета

ТОП / АНТИТОП уязвимостей декабря и января

Эксперты СайберОК снова полезли туда, куда по доброй воле никто не ходит — в лог-болото и разведанные СКИПА. Не из праздного любопытства, а чтобы разобраться! Как водится, прошлись по инстансам, сверили телеметрию и посмотрели на вещи трезво: какие уязвимости действительно могут испортить жизнь Рунету, а какие просто эффектно всплывали в новостных лентах и так же быстро исчезали.

Исследования, приведённые в статье, выполнялись исключительно на уровне внешнего периметра в сети Интернет и могут выявлять только те векторы и артефакты, которые доступны извне (публичные сервисы, открытые порты, публичные конфигурации и метаданные). Эти результаты не отображают состояние внутренней инфраструктуры, сетевой сегментации, конфигураций на хостах, контроля привилегий или телеметрии. Для корректной и полной оценки уровня безопасности нужно обязательно провести внутренние аудиторские проверки.

ТОП: Высокий риск + высокий охват в Рунете



* CybVSS – CyberOK Vulnerability Scoring System – метрика, разработанная нашими экспертами. Используется для быстрой оценки уязвимости на основе многих данных о ней.

Рассчитывается по формуле

$CybVSS = latest_cvss_bs^2 * spread * exploitability * mentions * k_kev$, где:

- *latest_cvss_bs* — базовая оценка CVSS последней версии;
- *spread* — распространенность (количество хостов, затронутых уязвимостью);
- *exploitability* — эксплуатируемость (количество эксплойтов);
- *mentions* — цитируемость (количество постов);
- *k_kev* — наличие факта эксплуатации уязвимости.

С точки зрения математического анализа, основное внимание уделяется уязвимостям, чье значение CybVSS превышает 100. Такие уязвимости классифицируются как трендовые, что подразумевает их высокую значимость и потенциальную актуальность в контексте потенциальных эксплуатаций злоумышленниками.

1. Обход аутентификации в telnetd / Press -f to pay respect (CVE-2026-24061)

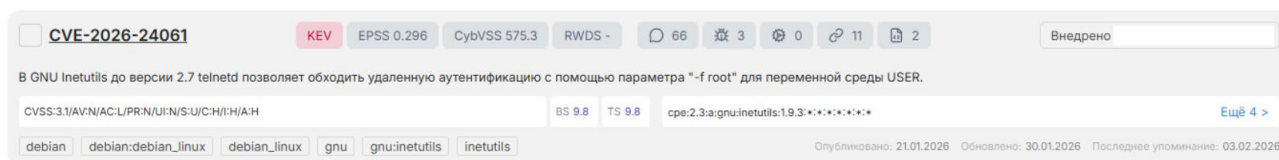
CVSS: 9.8 | KEV: да | Упоминания СКИПА: 60+ | CybVSS: 566.7

Масштаб: На радарх СКИПА мы наблюдаем более 500 инстансов telnetd по косвенным признакам.

Описание: В GNU Inetutils до версии 2.7 telnetd позволяет обходить удаленную аутентификацию с помощью параметра "-f root" для переменной среды USER.

Что по факту: Классика не стареет и эта уязвимость — яркий тому пример. Подобные векторы (аргумент -f для форсированного входа без пароля) считались вымершими еще в эпоху модемного интернета. Есть высокий риск автоматизированных атак, несмотря на то, что определить точное количество подверженных инстансов неинвазивными методами затруднительно. Эксперты уже фиксируют успешные эксплуатации и попытки загрузки вредоносного ПО на взломанные экземпляры.

Вердикт: Несмотря на небольшое количество потенциально уязвимых хостов на внешнем периметре, существует высокий риск эксплуатации критической уязвимости в закрытом контуре. Telnetd может быть предустановлен на промышленном оборудовании.



2. MongoDB Server / Сжатие с побочным эффектом (CVE-2025-14847)

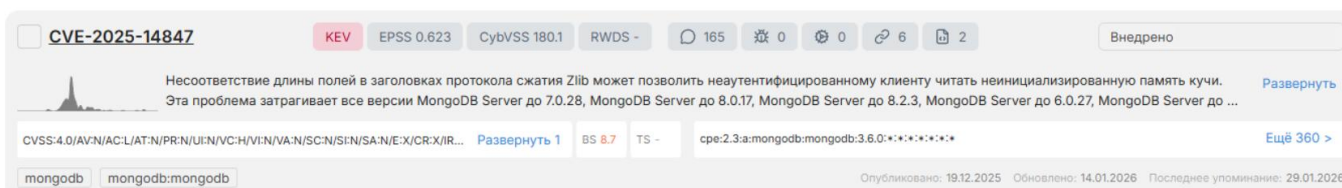
CVSS: 8.8 | KEV: нет | Упоминания СКИПА: 60+ | CybVSS: 180.1

Масштаб: На радарх СКИПА мы наблюдаем ~6250 инстансов MongoDB Server, из которых потенциально уязвимы 98%.

Описание: В системе управления базами данных MongoDB выявлена уязвимость, связанная с некорректной обработкой размеров сжатых данных при использовании алгоритма zlib. Эксплуатация уязвимости позволяет неавторизованным пользователям несанкционированно получить доступ к конфиденциальной информации.

Что по факту: PoC публично доступен.

Вердикт: Автоматизированная атака маловероятна из-за особенностей эксплуатации, но риск целевых атак сохраняется. Срочно обновите систему!



3. n8n / ni8mare (CVE-2026-21858, а также CVE-2025-68613 / CVE-2025-68668)

CVSS: 10 | KEV: нет | Упоминания СКИПА: 50+ | CybVSS: 369

Масштаб: СКИПА фиксирует ~12300 доступных экземпляров n8n, из которых потенциально уязвимы хотя бы к одной из уязвимостей 54%.

Описание: В версиях до 1.65.0 и после 1.121.0 злоумышленник может получить доступ к файлам на базовом сервере через выполнение рабочих процессов на основе форм. Если рабочий процесс уязвим, неаутентифицированный удаленный атакующий может получить доступ к конфиденциальной информации, что может привести к компрометации системы. Проблема решена в версии 1.121.0.

Что по факту: Демонстрация атаки доступна для публичного ознакомления, однако её успешное проведение требует предварительной подготовки. Хотя риск автоматизированных атак минимизирован, полностью исключить его нельзя.

Вердикт: Срочно обновите систему!

CVSS: 10 | KEV: нет | Упоминания СКИПА: 50+ | CybVSS: 369

Сортировка: Дата обновления, Дата публикации, Base Score, Количество упоминаний, Важные упоминания, EPSS, CybVSS, Распространенность, Эксплоиты

1 угроза из 15 источников

CVE-2026-21858 EPSS 0.054 CybVSS 370.9 RWDS - 49 3 0 2 2

n8n — это платформа автоматизации рабочих процессов с открытым исходным кодом. Версии, начинающиеся с 1.65.0 и ниже 1.121.0, позволяют злоумышленнику получить доступ к файлам на базовом сервере посредством выполнения определенных рабочих процессов на основе форм. Уязвимый рабочий процесс может предоставить доступ неаутентифицированному ...

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/H:N/A:N BS 10 TS 10 cpe:2.3:a:n8n:n8n:1.100.0:*:*:*node.js:*

n8n n8n:n8n Опубликовано: 08.01.2026 Обновлено: 16.01.2026 Последнее упоминание: 02.02.2026

4. Apache Tika / PDF, который слишком много знал (CVE-2025-66516)

CVSS: 10 | KEV: нет | Упоминания СКИПА: 30+

Масштаб: На радарх СКИПА мы наблюдаем ~200 экземпляров Apache Tika, из которых потенциально уязвимы ~97%.

Описание: В модулях Apache Tika (tika-core, tika-pdf-module, tika-parsers) обнаружена критическая уязвимость XXE, позволяющая злоумышленнику внедрять внешние XML-сущности через специально созданный файл XFA в PDF.

Что по факту: На момент исследования публичных PoC не было. Сейчас существует несколько репозиторий с потенциальными демонстрациями эксплуатации, но их достоверность не подтверждена.

Вердикт: Проверить внешние активы, выполнить обновление.

🔍 CVE-2025-66516 ✕ Найти

Сортировка
 ↑ Дата обновления ↓ Дата публикации ↓ Base Score ↓ Количество упоминаний ↓ Важные упоминания ↓ EPSS ↓ CYBVSS ↓ Распространенность
 ↓ Эксплоиты

1 угроза из 15 источников ⓘ

CVE-2025-66516 EPSS 0.026 CybVSS 0 RWDS - 32 1 0 2 2

Критическая уязвимость XXE в модулях Apache Tika tika-core (1.13-3.2.1), tika-pdf-module (2.0.0-3.2.1) и tika-parsers (1.13-1.28.5) на всех платформах позволяет злоумышленнику выполнить внедрение внешней сущности XML через специально созданный XFA-файл внутри PDF-файла. Эта уязвимость CVE покрывает ту же уязвимость, что и CVE-2025-54988. Однако эта ... [Развернуть](#)

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:X/CR:X/IR... [Развернуть 1](#) BS 10 TS - cpe:2.3:a:apache:tika:1.13:*:*:*:*:*:* [Ещё 46 >](#)

vendor-advisory related apache apache:tika tika

Опубликовано: 04.12.2025 Обновлено: 30.12.2025 Последнее упоминание: 30.12.2025

5. React Server Components / DoS (CVE-2026-23864)

CVSS: 7.5 | KEV: нет | Упоминания СКИПА: 10+ | CybVSS: 41.9

Масштаб: СКИПА фиксирует ~26 000 доступных инстансов React Server Components, из которых потенциально уязвимы 33%.

Описание: В компонентах React Server Components выявлены уязвимости типа «отказ в обслуживании», затрагивающие пакеты react-server-dom-parcel, react-server-dom-turbopack и react-server-dom-webpack. Уязвимости эксплуатируются при отправке специально сформированных HTTP-запросов к точкам Server Function, что может привести к сбоям, нехватке памяти или чрезмерному использованию CPU. Риски зависят от уязвимого участка кода, конфигурации и самого приложения.

Что по факту: Фундаментальная асимметрия в парсере react-server-dom. POST-запрос вызывает неконтролируемую рекурсию. Итог: 100% CPU, Memory Spike и падение Node.js по ООМ. Эксплуатация возможна без авторизации. Фиксируются попытки эксплуатации уязвимости в "дикой природе".

Вердикт: Срочно обновить React и Next.js, настроить WAF.

🔍 CVE-2026-23864 ✕ Найти

Сортировка
 ↑ Дата обновления ↓ Дата публикации ↓ Base Score ↓ Количество упоминаний ↓ Важные упоминания ↓ EPSS ↓ CYBVSS ↓ Распространенность
 ↓ Эксплоиты

1 угроза из 15 источников ⓘ

CVE-2026-23864 EPSS 0.008 CybVSS 41.9 RWDS - 11 0 0 1 2

В компонентах React Server Components существует множество уязвимостей типа «отказ в обслуживании», затрагивающих следующие пакеты: react-server-dom-parcel, react-server-dom-turbopack, react-server-dom-webpack. Уязвимости активируются при отправке специально сформированных HTTP-запросов к конечным точкам Server Function и могут привести к сбоям ... [Развернуть](#)

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/N/I:N/A:H BS 7.5 TS 7.5 -

Опубликовано: 26.01.2026 Обновлено: 27.01.2026 Последнее упоминание: 29.01.2026

6. 1С-Битрикс / Path Traversal, Sensitive Data Exposure (BDU:2025-16324 / BDU:2025-16325 / BDU:2025-16349 / BDU:2025-16350)

CVSS: 7.5 | KEV: нет | Упоминания СКИПА: 5+ | СОК: да

Масштаб: СКИПА фиксирует ~1 500 000 доступных инстансов 1С-Битрикс, из которых потенциально уязвимы 3% (45 000 хостов!).

Описание: Исследователь СайберОК Роберт Торосян обнаружил несколько уязвимостей в популярных сторонних плагинах Eolutions, размещенных в каталоге решений 1С-Битрикс: Управление сайтом. Уязвимости в плагинах связаны с неверным ограничением имени пути к каталогу. Эксплуатация уязвимостей позволяет нарушителю, действующему удалённо, получить несанкционированный доступ к защищаемой информации.

Что по факту: Большая распространенность в РУ сегменте. Публичного PoC нет, вероятность автоматизированных атак снижена.

Вердикт: При наличии данного плагина на инстансах с 1С-Битрикс требуется обновление!

The screenshot shows a search interface for vulnerabilities. At the top, there is a search bar with the query 'BDU:2025-16324' and a 'Найти' button. Below the search bar, there are several filter buttons: 'Дата обновления', 'Дата публикации', 'Base Score', 'Количество упоминаний', 'Важные упоминания', 'EPSS', 'CybVSS', and 'Распространенность'. There is also a 'Сортировка' dropdown and an 'Эксплоиты' button. The main content area shows a single result for 'BDU:2025-16324'. The result card includes a title 'Уязвимость плагина «Экспорт/Импорт товаров в Excel» связана с неверным ограничением имени пути к каталогу. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, получить несанкционированный доступ к защищаемой информации'. Below the title, there is a CVSS score 'CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N' and a 'Развернуть 2' button. At the bottom right of the card, it says 'Опубликовано: 19.12.2025', 'Обновлено: Нет', and 'Последнее упоминание: Нет'.

7. GeoServer / XXE (CVE-2025-58360)

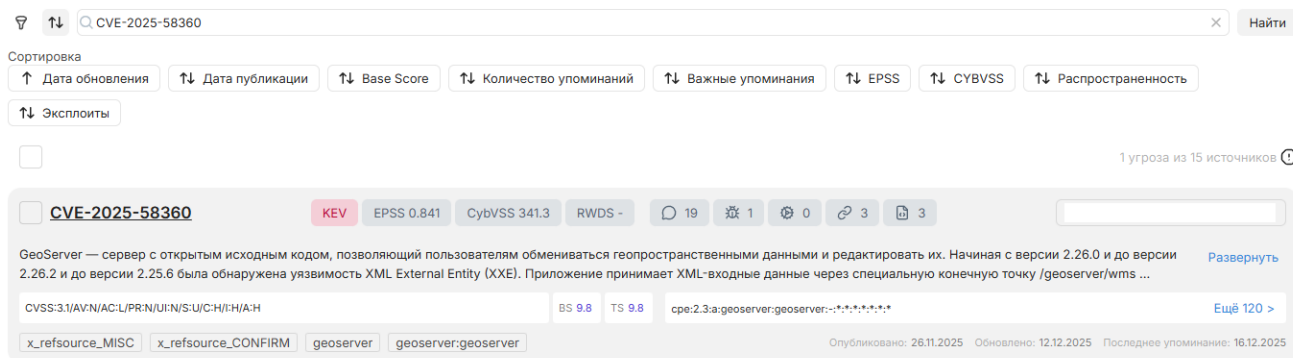
CVSS: 9.8 | KEV: да | Упоминания СКИПА: 19+ | CybVSS: 341.3

Масштаб: СКИПА наблюдает в Рунете ~200 активных инстансов, из которых 50%+ потенциально уязвимы.

Описание: GeoServer — сервер с открытым исходным кодом для обмена геопространственными данными, имел уязвимость XML External Entity (XXE) в версиях 2.26.0-2.26.2 и 2.25.6. Уязвимость позволяла злоумышленникам определять внешние сущности через незащищенную конечную точку /geoserver/wms

Что по факту: ПО с достаточно высоким уровнем критичности. На момент исследования в Интернет имелся публично доступный валидный PoC.

Вердикт: Требуется срочное обновление, GeoServer также подвержен более серьезным уязвимостям, например, Remote Code Execution.



🔍 CVE-2025-58360

Сортировка
 ↑ Дата обновления | ↓ Дата публикации | ↓ Base Score | ↑ Количество упоминаний | ↑ Важные упоминания | ↓ EPSS | ↓ CYBVSS | ↓ Распространенность

↑ Эксплоиты

1 угроза из 15 источников ⓘ

CVE-2025-58360 KEV EPSS 0.841 CybVSS 341.3 RWDS - 19 1 0 3 3

GeoServer — сервер с открытым исходным кодом, позволяющий пользователям обмениваться геопространственными данными и редактировать их. Начиная с версии 2.26.0 и до версии 2.26.2 и до версии 2.25.6 была обнаружена уязвимость XML External Entity (XXE). Приложение принимает XML-входные данные через специальную конечную точку /geoserver/wmts ... [Развернуть](#)

CVSS:3.1(AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H) BS 9.8 TS 9.8 cpe:2.3.a:geoserver:geoserver-:*:*:*:*:*.* [Ещё 120 >](#)

x_refsource_MISC | x_refsource_CONFIRM | geoserver | geoserver:geoserver

Опубликовано: 26.11.2025 Обновлено: 12.12.2025 Последнее упоминание: 16.12.2025

8. Fortinet / Множественные уязвимости в продуктах Fortinet (CVE-2025-59718 / CVE-2026-24858 / CVE-2025-59719 / CVE-2020-12812)

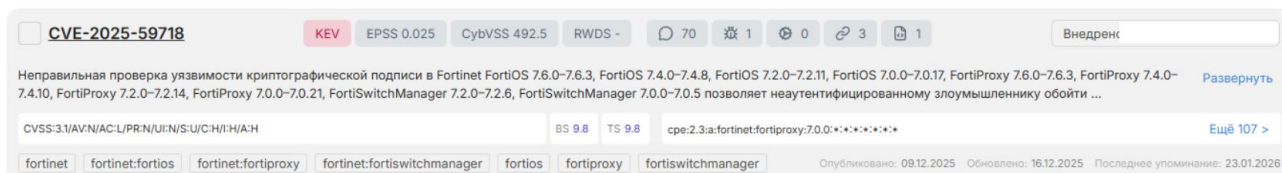
CVSS: 9.8 | KEV: да | Упоминания СКИПА: 190+ (в сумме)

Масштаб: СКИПА фиксирует 2400 функционирующих экземпляров FortiOS и FortiWeb. Из них более 50% потенциально уязвимы хотя бы к одной из выявленных проблем безопасности.

Описание: Данные уязвимости в различных версиях продуктов Fortinet (FortiOS, FortiProxy, FortiManager и др.) связаны с критическими недостатками в механизмах проверки подписей SAML, некорректной обработкой регистров имен пользователей и архитектурными ошибками аутентификации через FortiCloud SSO. Эти бреши позволяют злоумышленникам обходить проверку подлинности, включая двухфакторную аутентификацию, и получать несанкционированный доступ к устройствам и системам единого входа.

Что по факту: ПО с высоким уровнем критичности должно быть защищено от прямого доступа из внешних сетей. Однако, в силу особенностей работы VPN-шлюзов и межсетевых экранов, их часто необходимо делать доступными извне. Это, в сочетании с публично доступными эксплоитами, делает такие хосты приоритетными целями для автоматизированных атак.

Вердикт: Для обеспечения безопасности необходимо незамедлительно обновить затронутые компоненты до актуальных исправленных версий, указанных производителем.



🔍 CVE-2025-59718

KEV EPSS 0.025 CybVSS 492.5 RWDS - 70 1 0 3 1

Внедрен

Неправильная проверка уязвимости криптографической подписи в Fortinet FortiOS 7.6.0-7.6.3, FortiOS 7.4.0-7.4.8, FortiOS 7.2.0-7.2.11, FortiOS 7.0.0-7.0.17, FortiProxy 7.6.0-7.6.3, FortiProxy 7.4.0-7.4.10, FortiProxy 7.2.0-7.2.14, FortiProxy 7.0.0-7.0.21, FortiSwitchManager 7.2.0-7.2.6, FortiSwitchManager 7.0.0-7.0.5 позволяет неаутентифицированному злоумышленнику обойти ... [Развернуть](#)

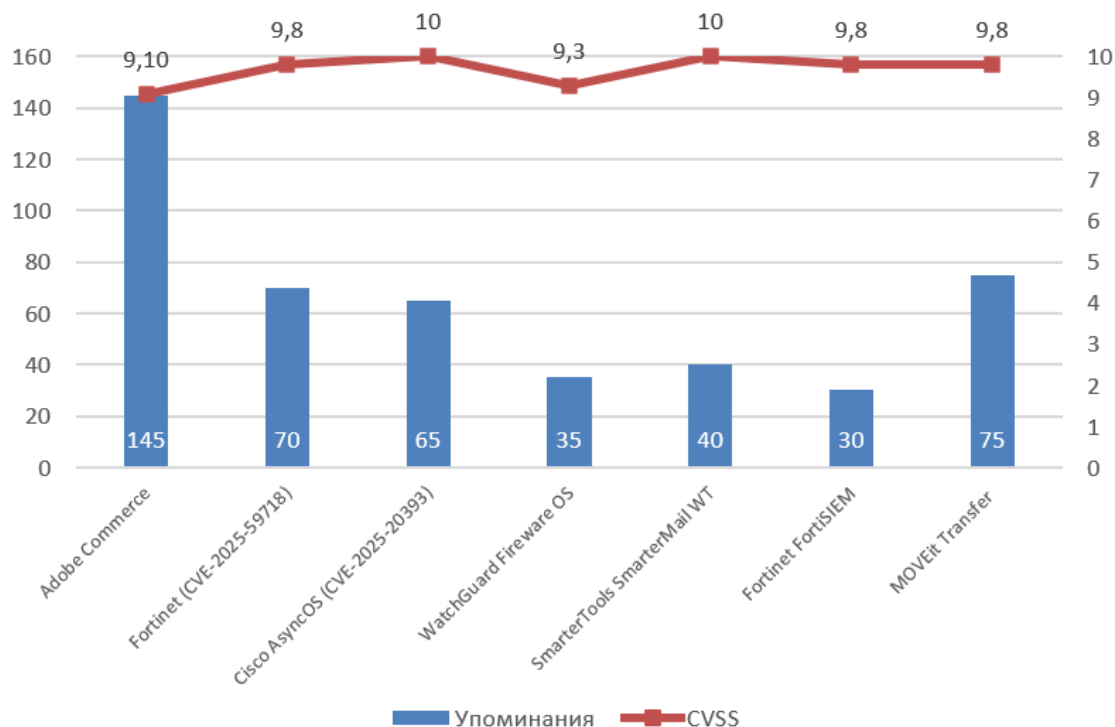
CVSS:3.1(AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H) BS 9.8 TS 9.8 cpe:2.3.a:fortinet:fortiproxy:7.0.0:*:*:*:*:*.* [Ещё 107 >](#)

fortinet | fortinet:fortios | fortinet:fortiproxy | fortinet:fortiswitchmanager | fortios | fortiproxy | fortiswitchmanager

Опубликовано: 09.12.2025 Обновлено: 16.12.2025 Последнее упоминание: 23.01.2026

АНТИТОП: Высокий риск + низкий охват в Рунете

АНТИТОП: Упоминания уязвимостей в Рунет и их CVSS



1. Adobe Commerce / Неправильная проверка входных данных (CVE-2025-54236)

CVSS: 9.1 | KEV: да | Упоминания СКИПА: 145+ | CybVSS: 497.4

Описание: Версии Adobe Commerce до 2.4.9-alpha2 подвержены уязвимости, связанной с неправильной проверкой вводимых данных. Злоумышленник может использовать эту уязвимость для перехвата сеанса, что увеличивает риск утечки конфиденциальной информации.

Что по факту: На радарх СКИПА на данный момент мы наблюдаем всего ~220 доступных извне хостов. Потенциально уязвимы 30%.

Вердикт: Критическая уязвимость, есть концептуальный PoC (то, как могла бы выглядеть уязвимость с логической точки зрения), но при этом распространенность на отечественном ландшафте низкая. Если имеете в своих активах, не стоит затягивать с обновлением — для эксплуатации не требуется взаимодействие с пользователем.

CVE-2025-54236 KEV EPSS 0.578 CybVSS 0 RWDS 4 153 1 0 4 3 Внедрено

Версии Adobe Commerce 2.4.9-alpha2, 2.4.8-p2, 2.4.7-p7, 2.4.6-p12, 2.4.5-p14, 2.4.4-p15 и более ранние подвержены уязвимости «Неправильная проверка входных данных». Злоумышленник может воспользоваться ею для захвата сеанса, что значительно повысит уровень конфиденциальности и целостности данных. ... Развернуть

CVSS:3.1(AV:N/AC:L/PR:N/UI:N/S:U/CN:1/H:A/N) BS 9.1 TS 9.1 cpe:2.3:a:adobe:commerce:2.4.4:-:*:*:*:*

adobe adobe:commerce adobe:commerce_b2b adobe:magento commerce commerce_b2b magento Опубликовано: 09.09.2025 Обновлено: 03.02.2026 Последнее упоминание: 04.02.2028

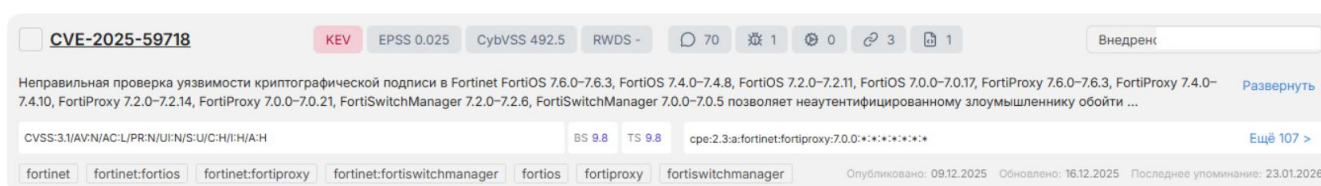
2. Fortinet / Обход авторизации (CVE-2025-59718)

CVSS: 9.8 | KEV: да | Упоминания СКИПА: 70+ | CybVSS: 492.5

Описание: В версиях Fortinet FortiOS и FortiProxy до 7.6.3, 7.4.10 и 7.2.14, а также в FortiSwitchManager до 7.2.6 и 7.0.5 обнаружена уязвимость в проверке криптографической подписи. Злоумышленник без авторизации может обойти систему единого входа в FortiCloud, используя специально сформированное ответное сообщение SAML.

Что по факту: В реалиях конца 2025 года, данные продукты Fortinet (за исключением FortiOS) встречаются крайне редко на внешнем периметре Рунета.

Вердикт: В Рунете нет живых инстансов.



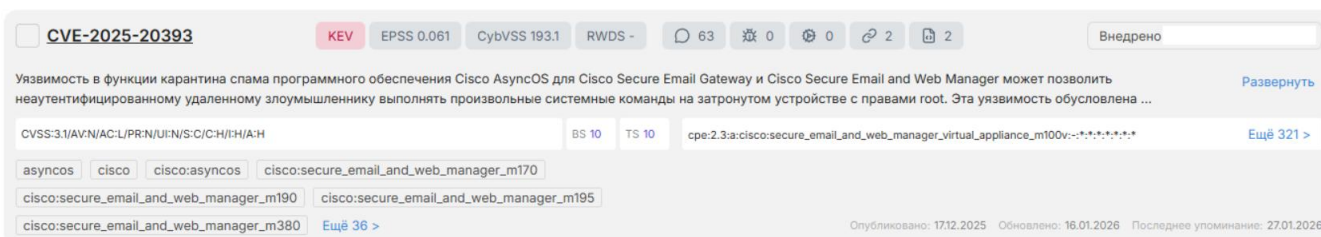
3. Cisco AsyncOS / Обход авторизации (CVE-2025-20393)

CVSS: 10 | KEV: да | Упоминания СКИПА: 65+ | CybVSS: 193.1

Описание: В системе фильтрации спама Cisco AsyncOS для устройств Cisco Secure Email Gateway и Cisco Secure Email and Web Manager выявлена критическая уязвимость. Злоумышленники, не имеющие аутентификации, могут использовать её для выполнения команд с правами администратора на затронутом оборудовании. Проблема заключается в недостаточной проверке HTTP-запросов при карантинировании спама. Злоумышленник способен эксплуатировать уязвимость, отправив на устройство специально сформированный HTTP-запрос. Успешная атака позволяет выполнять произвольные команды в базовой операционной системе от имени суперпользователя.

Что по факту: Среди внешних активов однозначно можно задетектировать только AsyncOS. Для уязвимости нет публично доступных PoC'ов.

Вердикт: Всего в Рунете мы наблюдаем до 20 доступных хостов, из которых 15% потенциально уязвимы.



4. WatchGuard Fireware OS / RCE (CVE-2025-14733)

CVSS: 9.3 | KEV: нет | Упоминания СКИПА: 35+ | CybVSS: 145.5

Описание: В WatchGuard Fireware OS обнаружена уязвимость, позволяющая удалённому неаутентифицированному злоумышленнику выполнять произвольный код при записи за пределы допустимого диапазона. Уязвимость распространяется на VPN для мобильных пользователей, использующих IKEv2 и на VPN для филиалов с IKEv2 и динамическим шлюзом. Она затрагивает следующие версии Fireware OS:

- от 11.10.2 до 11.12.4_Update1;
- от 12.0 до 12.11.5;
- от 2025.1 до 2025.1.3.

Что по факту: На момент исследования публичный PoC в сети недоступен.

Вердикт: В Рунете насчитывается до 180 хостов, 100% потенциально уязвимы. На момент исследования публично доступных PoC не выявлено, что снижает вероятность массовых и автоматизированных атак.

Сортировка
↑ Дата обновления ↓ Дата публикации ↓ Base Score ↓ Количество упоминаний ↓ Важные упоминания ↓ EPSS ↓ CYBVSS ↓ Распространенность
↓ Эксплоиты

1 угроза из 15 источников

CVE-2025-14733 KEV EPSS 0.432 CybVSS 145.5 RWDS - 37 0 0 2 1

Уязвимость, связанная с записью за пределы допустимого диапазона, в WatchGuard Fireware OS может позволить удаленному неаутентифицированному злоумышленнику выполнить произвольный код. Эта уязвимость затрагивает как VPN для мобильных пользователей с IKEv2, так и VPN для филиалов, использующих IKEv2 при настройке с динамическим шлюзом. [Развернуть](#)

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR... [Развернуть 1](#) BS 9.3 TS - cpe:2.3h:watchguard:firebox_m270-*:*:*:*:* [Ещё 151 >](#)

firebox_m270 firebox_m290 firebox_m370 firebox_m390 firebox_m440 firebox_m4600 firebox_m470 [Ещё 62 >](#)

Опубликовано: 19.12.2025 Обновлено: 23.12.2025 Последнее упоминание: 28.01.2026

5. SmarterTools SmarterMail WT / Почта с сюрпризом (CVE-2025-52691)

CVSS: 10 | KEV: да | Упоминания СКИПА: 40+ | CybVSS: 173.1

Описание: Успешная эксплуатация уязвимости в системе SmarterTools SmarterMail WT позволяет неавторизованному злоумышленнику загружать произвольные файлы в любое место на почтовом сервере, потенциально обеспечивая удаленное выполнение кода.

Что по факту: В открытом доступе находятся Proof-of-Concept и nuclei-шаблоны, что свидетельствует о наличии у злоумышленников эффективных инструментов для проведения атак. Это создает предпосылки для повышения вероятности автоматизированных атак. Хорошая новость: ПО специфичное, эксперты СайберОК обнаружили всего 2 потенциально подходящих под описание и классификацию хостов на просторах Рунета.

Вердикт: Страшно, но не в реалиях Российского сегмента.

6. Fortinet FortiSIEM / Специально сконструированный TCP (CVE-2025-64155)

CVSS: 9.8 | KEV: нет | Упоминания СКИПА: 30+ | CybVSS: 251.8

Описание: Некорректная нейтрализация специфических команд операционной системы в уязвимостях продуктов Fortinet FortiSIEM версий 7.4.0, 7.3.0–7.3.4, 7.1.0–7.1.8, 7.0.0–7.0.4 и 6.7.0–6.7.10 создаёт риск для несанкционированного выполнения команд или кода через специально сконструированные TCP-запросы.

Что по факту: На момент исследования в сети обнаружен публичный PoC, его достоверность не была проверена. В РУ-сегменте доступные извне хосты не обнаружены.

Вердикт: В Рунете не встречается на внешнем периметре.

7. MOVEit Transfer/ Гроза интернета, но не Рунета (CVE-2023-34362)

CVSS: 9.8 | KEV: да | Упоминания СКИПА: 75+ | CybVSS: 614.5

Описание: В MOVEit Transfer до версий 2021.0.6, 2021.1.4, 2022.0.4, 2022.1.5 и 2023.0.1 обнаружена уязвимость SQL-инъекции. Злоумышленник может получить доступ к базе данных, вывести информацию и выполнить SQL-операторы. Уязвимость эксплуатируется через HTTP или HTTPS начиная с мая 2023 года. Подвержены все версии до указанных, включая старые.

Что по факту: Существует общедоступный PoC и пускеш-шаблоны, которые могут использоваться для автоматизированных атак.

Вердикт: Программное обеспечение данного типа не представлено в открытом доступе в российском сегменте Интернет.

The screenshot shows a search interface for CVE-2023-34362. At the top, there is a search bar with the query 'CVE-2023-34362' and a 'Найти' button. Below the search bar, there are sorting options: 'Дата обновления', 'Дата публикации', 'Base Score', 'Количество упоминаний', 'Важные упоминания', 'EPSS', 'CYBVSS', and 'Распространенность'. A 'Эксплоиты' button is also present. The main content area displays the CVE ID 'CVE-2023-34362' with a 'KEV' tag, an EPSS score of 0.943, and other identifiers like 'CybVSS 614.5' and 'RWDS -'. It also shows 73 mentions, 50 CVEs, 0 exploits, 4 references, and 2 advisories. The description states: 'В процессе MOVEit Transfer до 2021.0.6 (13.0.6), 2021.1.4 (13.1.4), 2022.0.4 (14.0.4), 2022.1.5 (14.1.5) и 2023.0.1 (15.0.1) в веб-приложении MOVEit Transfer была обнаружена уязвимость SQL-инъекции, которая может позволить неаутентифицированному злоумышленнику получить доступ к базе данных MOVEit Transfer. В зависимости от используемого ядра базы данных ...'. The CVSS score is 3.1 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) with a Base Score of 9.8 and a Temporal Score of 9.8. The CPE is 'cpe:2.3:a:progress:moveit_cloud:-:*:*:*:*:*'. There are buttons for 'VDB Entry', 'Vendor Advisory', 'Exploit', 'Third Party Advisory', 'moveit_cloud', 'moveit_transfer', and 'progress'. The page was published on 02.06.2023, updated on 27.10.2025, and the last mention was on 27.10.2025.

Выводы

Декабрь–январь снова доказали прописную истину: важна не цифра CVSS, а то, насколько ПО распространено в Рунете, доступно извне и реально эксплуатируемо.

Обновлять нужно всё, но в первую очередь — то, что стоит на периметре, широко используется и имеет подтверждённые векторы эксплуатации. Это и есть практическая кибергигиена.

Пользуясь случаем, приглашаем вас в наш телеграм-канал, где мы регулярно рассказываем о самых показательных находках.