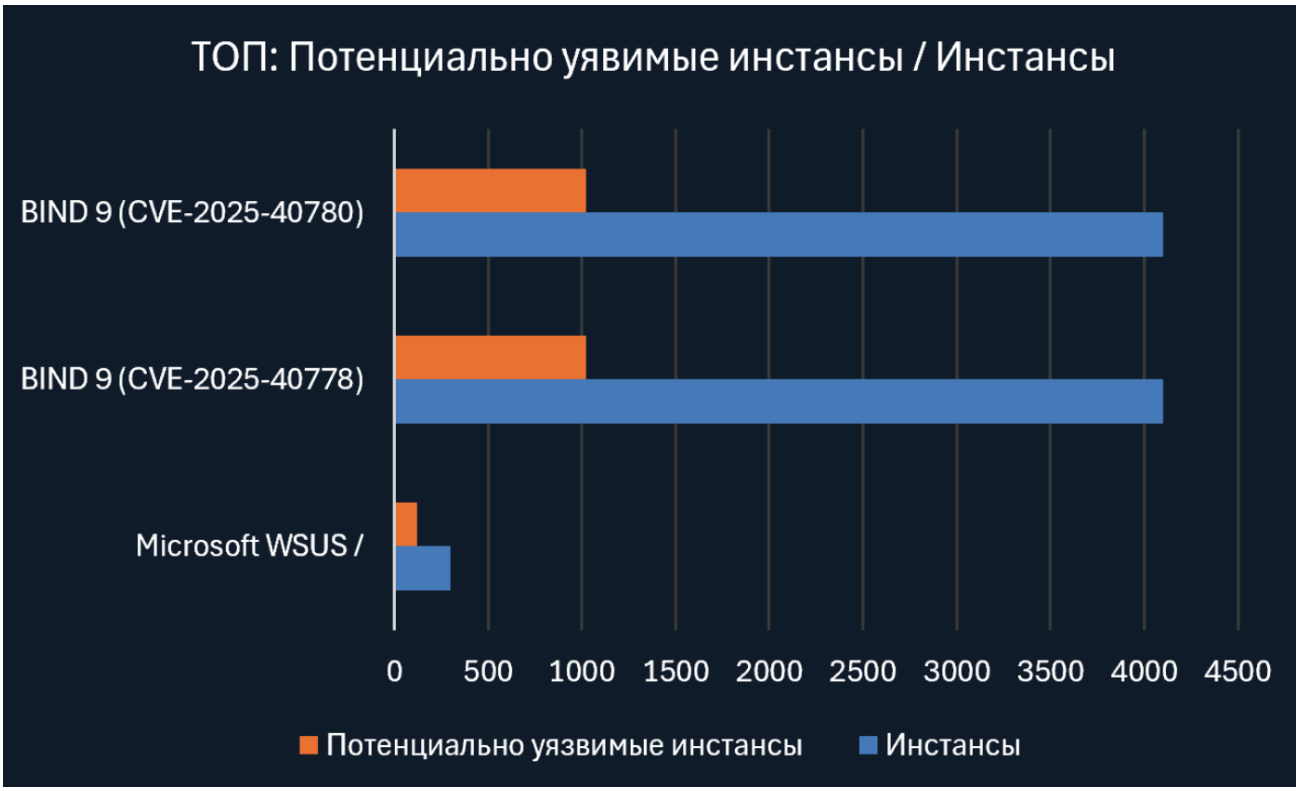
www.cyberok.ru
info@cyberok.ru
+7 (495) 137-7337

РУНЕТ В СТРАНЕ КОШМАРОВ: ТОП/АНТИТОП УЯЗВИМОСТЕЙ ОКТЯБРЯ

Как вы провели Хэллоуин? Вот мы в СайберОК качественно повеселились и попугались, ведь наши эксперты-охотники на привидений до самого рассвета рыскали по внешнему периметру Рунета и вытаскивали на свет главных монстров октября – как новых, так и хорошо забытых старых.

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 аудирование.

ТОП: Высокий риск + высокий охват в Рунете



1. RCE в Microsoft WSUS / Обновить нельзя эксплуатировать (CVE-2025-59287)

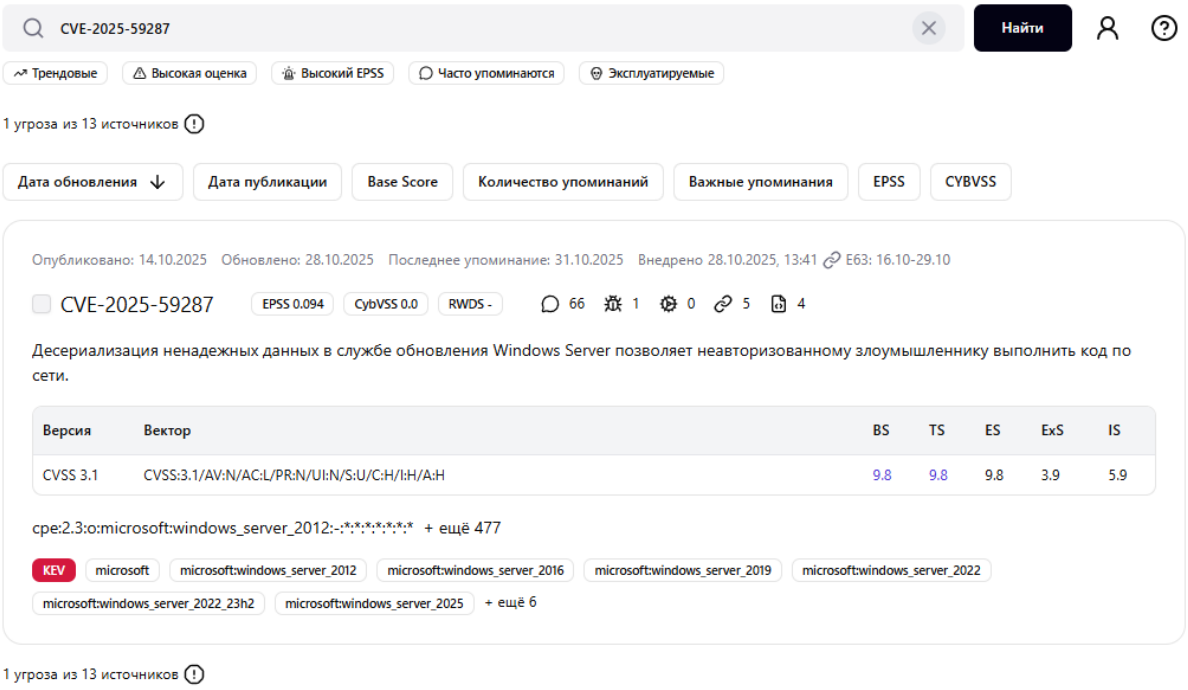
CVSS: 9.8 | KEV: да

Масштаб: На радарах СКИПА мы наблюдаем ~300 инстансов Microsoft WSUS SimpleAuthWebService, из которых уязвимы около 40%.

Описание: Критическая уязвимость RCE в службах обновления Microsoft Windows Server (WSUS). Проблема вызвана небезопасной десериализацией данных AuthorizationCookie с помощью BinaryFormatter в методе EncryptionHelper.DecryptData() . Уязвимость позволяет злоумышленнику без аутентификации выполнить удаленный код с привилегиями SYSTEM, отправив вредоносные зашифрованные файлы cookie на конечную точку GetCookie().

Что по факту: Критическое ПО, успешные кейсы эксплуатации уязвимости в дикой природе уже зафиксированы.

Вердикт: Серьёзная уязвимость с KEV, срочно обновить.



2. BIND 9 / Cache Poisoning (CVE-2025-40778)

CVSS: 8.6 | KEV: нет

Масштаб: На радарах СКИПА мы наблюдаем ~4.100 инстансов BIND-9, из которых уязвимы около 25%.

Описание: При определённых обстоятельствах BIND недостаточно валидирует записи в ответах, что позволяет злоумышленнику внедрять поддельные данные в кэш.

Что по факту: Публичный PoC доступен, злоумышленник способен внедрять поддельные записи в кэш уязвимого резолвера, что приведёт к подмене DNS-ответов для всех его клиентов (редирект трафика, подмена адресов сервисов и т.п.). Потенциально масштабная атака на незащищённые инстансы.

Вердикт: Серьёзная уязвимость — обновить BIND немедленно. До патча: ограничить рекурсивный доступ (ACL), запретить рекурсию на публичных серверах, включить/проверить DNSSEC на критичных зонах, мониторить нестандартные RRset в кэше и логи ответов.

3. BIND 9 / Повышаем градус эксплуатации (CVE-2025-40780)

CVSS: 8.6 | KEV: нет

Масштаб: На радарах СКИПА мы наблюдаем ~4.100 инстансов BIND-9, из которых уязвимы около 25%.

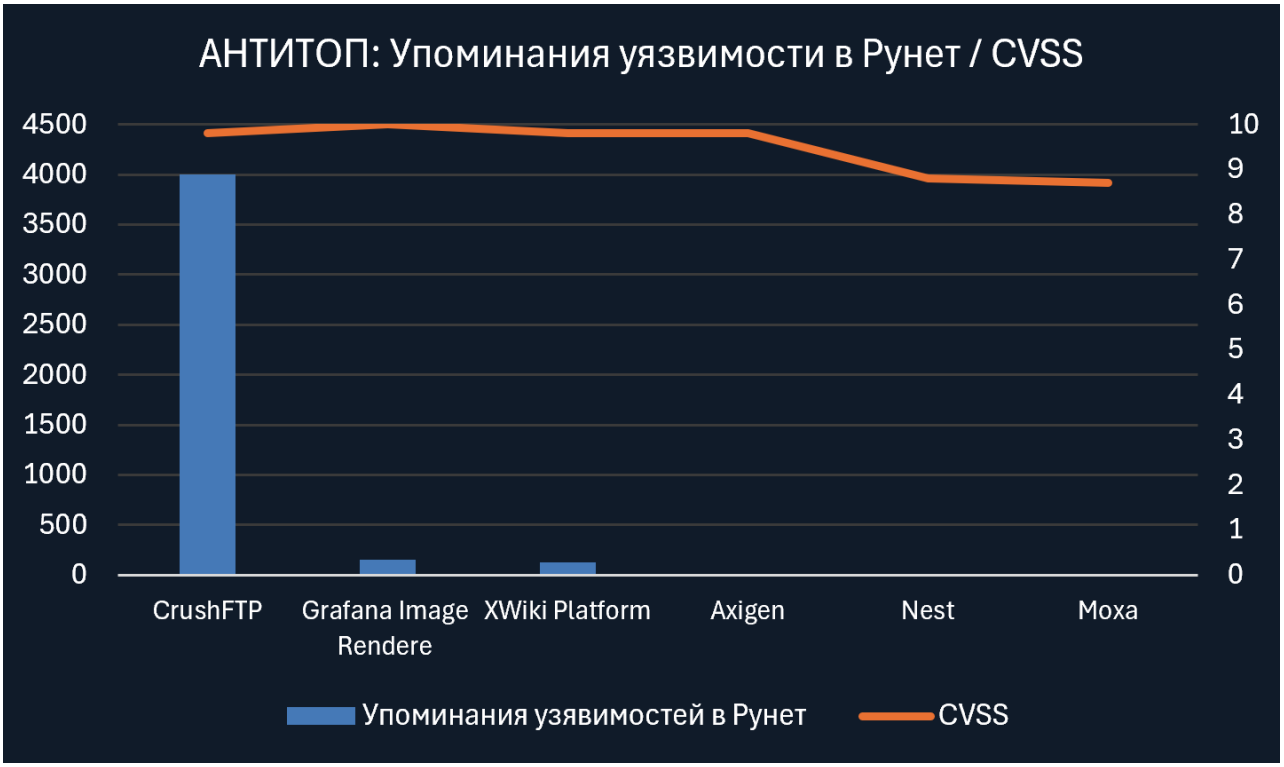
Описание: Ослабление энтропии генератора псевдослучайных значений, используемого для формирования transaction ID и source port. Сужение пространства возможных комбинаций значительно повышает вероятность успешного угадывания полей, по которым резолвер сопоставляет ответы с запросами.

Что по факту: В сочетании с уязвимостью в обработке unsolicited RRs (CVE-2025-40778) сниженная случайность делает приёмы форженных ответов гораздо более надёжными — публичный PoC показывает практическую пригодность этой техники. Риск — массовая подмена кэша при таргетинге уязвимых резолверов.

Вердикт: Критично — поставить патч как можно скорее. До патча: по возможности ограничить исходящие/входящие порты, использовать NAT/порт-рандомизацию на сетевом уровне, включить DNSSEC, отслеживать аномалии в совпадениях transaction ID/port и рассмотреть перевод критичных клиентов на надёжные внешние резолверы.

www.cyberok.ru
info@cyberok.ru
+7 (495) 137-7337

АНТИТОП: Высокий риск + низкий охват в Рунете



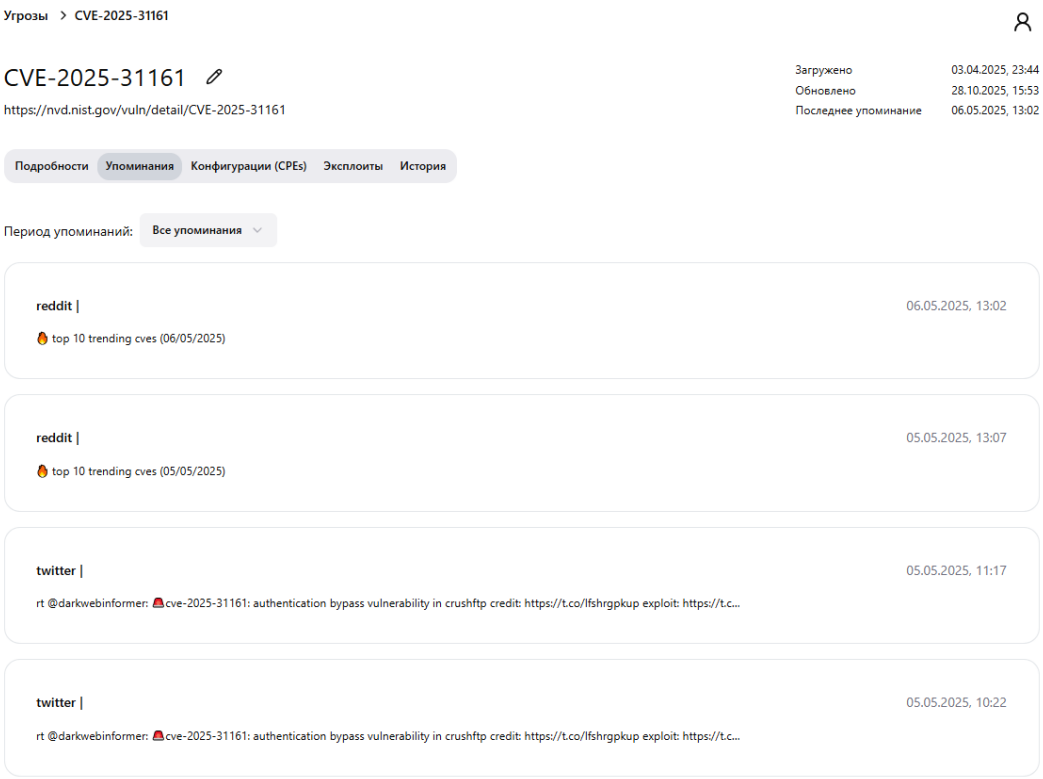
1. CrushFTP / Гонка за креслом admin (CVE-2025-31161)

CVSS: 9.8 | KEV: да | Упоминания СКИПА: 50+

Описание: CrushFTP версии до 10.8.4 / 11.x до 11.3.1 содержат уязвимость, позволяющую обойти аутентификацию и получить контроль над учётной записью crushadmin (если не используется прокси в DMZ). В методе авторизации AWS4-HMAC (S3-совместимой) в HTTP-компоненте FTP-сервера есть состояние гонки: сервер сначала вызывает login_user_pass() без запроса пароля — в этот момент сессия проходит проверку HMAC и считается аутентифицированной, а позднее сервер повторно проверяет пользователя.

Что по факту: В Рунете ~4000 экземпляров, есть публичный PoC и nuclei-шаблоны, но массовых кейсов эксплуатации подтвердить не удалось.

Вердикт: Серьёзная уязвимость, однако активность в Рунете не зафиксирована массово.



2. Axigen / Обход 2FA (CVE-2023-23566)

CVSS: 9.8 | KEV: нет | Упоминания СКИПА: 5+

Описание: Уязвимость в Axigen 10.3.3.52 даёт возможность обхода двухэтапной аутентификации, что позволяет злоумышленнику получить доступ к ящику при подключении учётной записи к стороннему веб-почтовому сервису.

Что по факту: Уязвимости подвержена версия приложения 10.3.3.52. В Рунете инстансы с данной версией не обнаружены.

Вердикт: Опасна по сути, но для РФ-сегмента не актуальна.

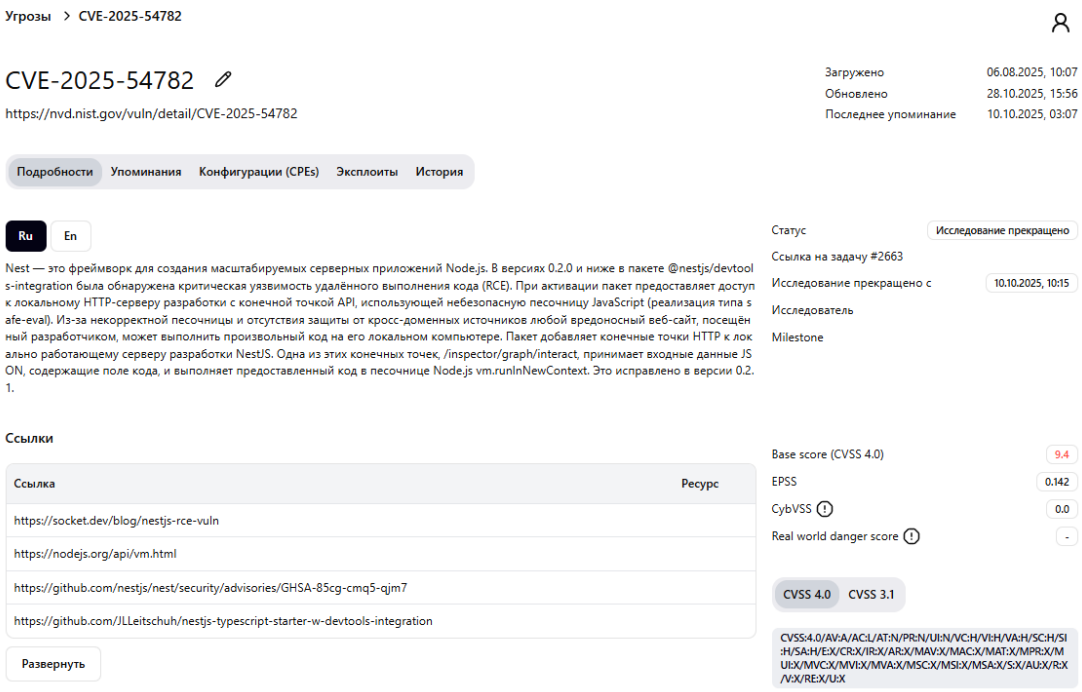
3. Nest RCE / Небезопасная песочница (CVE-2025-54782)

CVSS: 8.8 | KEV: нет | Упоминания СКИПА: 10+

Описание: В версиях ≤0.2.0 в пакете @nestjs/devtools-integration была обнаружена критическая уязвимость удалённого выполнения кода (RCE). При активации пакет предоставляет доступ к локальному HTTP-серверу разработки с конечной точкой API, использующей небезопасную песочницу JavaScript.

Что по факту: В РУ сегменте не обнаружено активных инстансов данного ПО.

Вердикт: Крайне низкий риск для Рунета.



4. Моха / Админская дверь без замка (CVE-2025-6892)

CVSS: 8.7 | KEV: нет | Упоминания СКИПА: 5+

Описание: В сетевых устройствах безопасности и маршрутизаторах Моха обнаружена уязвимость, связанная с некорректной авторизацией. Изъян в механизме аутентификации API позволяет получить несанкционированный доступ к защищённым конечным точкам API, включая те, которые предназначены для выполнения административных функций. Эта уязвимость может быть эксплуатирована после входа в систему аутентифицированного пользователя, поскольку система не может должным образом проверить контекст сеанса и не ограничивает привилегии должным образом.

Что по факту: Не удалось оценить распространенность в Рунете.

Вердикт: Крайне низкая вероятность активной эксплуатации в РУ сегменте.

5. Grafana Image Renderer RCE / Хардкод ключик (CVE-2025-11539)

*CVSS: 10 | KEV: нет | Упоминания СКИПА: 5+ | Cybvss: 54.6**

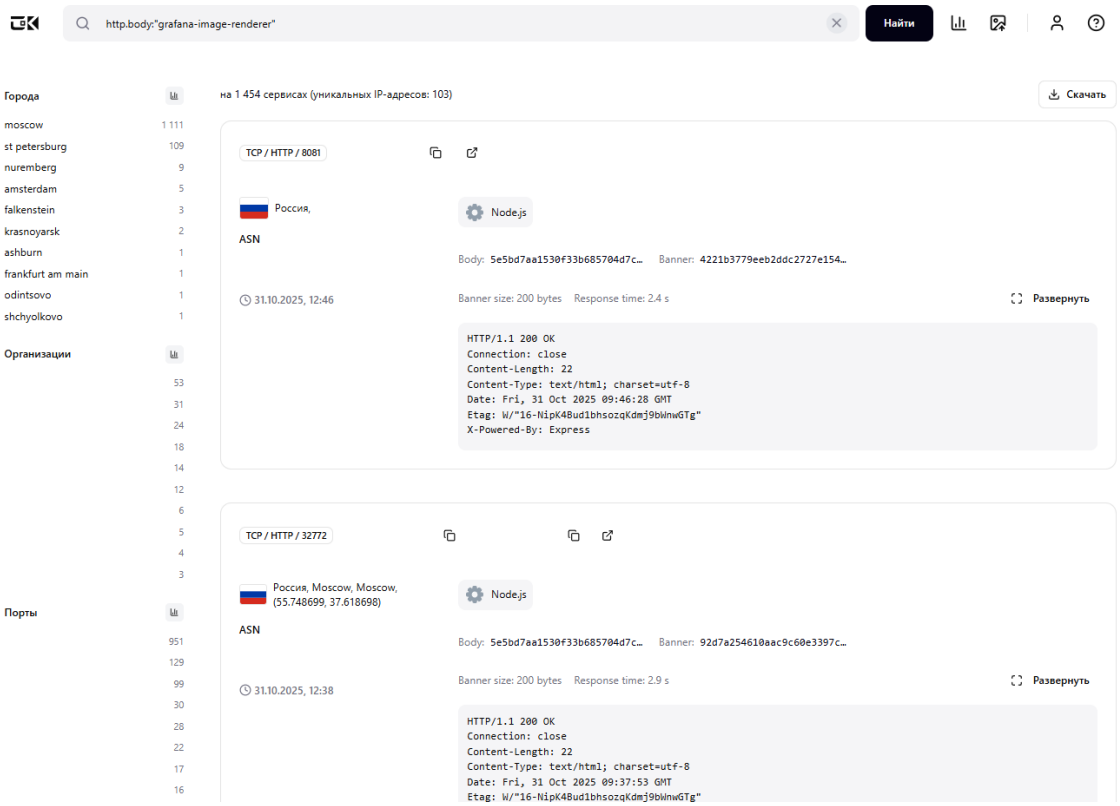
Масштаб: По данным СКИПА в Рунете работает ~150 активных инстансов, на момент исследования 100% из них уязвимы.

Описание: Grafana Image Renderer уязвим к удалённому выполнению кода из-за уязвимости записи произвольного файла. Это связано с тем, что конечная точка /render/csv не проходит проверку параметра filePath, что позволяет злоумышленнику сохранить общий объект в произвольном месте, а затем загрузить его процессом Chromium. Экземпляры уязвимы, если токен по умолчанию («authToken») не изменён или известен злоумышленнику.

Что по факту: Так как токен можно легко получить из исходного кода приложения, необходимо срочно изменить «authToken» на отличный от стандартного значения.

Вердикт: В Рунете такие экземпляры встречаются нечасто и не задерживаются на радарах.

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



6. XWiki Platform / RCE (CVE-2025-24893)

CVSS: 9.8 | KEV: да | Упоминания СКИПА: 30+

Описание: Уязвимость в XWiki реализуется через эндпоинт SolrSearch и позволяет любому пользователю выполнить произвольный код на хосте — без необходимости привилегий. Причина — недостаточная санитизация и/или некорректная обработка пользовательских параметров при формировании запросов/шаблонов для поискового компонента (Solr/механизмы шаблонизации).

Что по факту: В октябре был всплеск упоминаний уязвимости в публичных источниках. Эксперты СайберОК рассмотрели данную уязвимость в марте 2025 года: на момент исследования было приблизительно 7–8% уязвимых инстансов.

На сегодняшний день СКИПА видит примерно ~130 активных хостов с данным ПО в Рунете.

Вердикт: Уязвимость крайне опасная, но низкая распространённость в Рунете делает её менее приоритетной с точки зрения массовой эксплуатации — однако для подверженных инстансов обновление и внедрение компенсирующих мер остаются обязательными.

www.cyberok.ru
info@cyberok.ru
+7 (495) 137-7337

Выводы

Может быть самая страшная ночь в году и осталась позади, но уязвимостям сон не ведом.

1. Знайте свой сетевой периметр — освятите его светом инвентаризации и патчей.
2. Если по сети ползёт эксплойт — действуйте без промедления, пока тени не окутали ваши сервисы.
3. Даже редкие уязвимости могут ожить в полночь — удавите их прямо в колыбели.

И пусть ваши системы вздохнут спокойно под покровом обновлений.

В нашем телеграм-канале — кладовая знаний по кибербезопасности и мониторингу внешних атак. Заглядывайте.