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

КОМУ НА РУНЕТЕ ЖИТЬ ХОРОШО: ТОП/АНТИ-ТОП УЯЗВИМОСТЕЙ НОЯБРЯ

В ноябре мы снова погрузились в лог-болото и разведданные СКИПА, чтобы понять, какие уязвимости действительно опасны для Рунета, а какие просто всплыли в новостных лентах. Как обычно, прошлись по инстансам, сверили телеметрию, посмотрели, где есть PoC'ы, а где только шум.

По данным СКИПА за последние три месяца можно выделить следующие тенденции:

- Общее число уязвимостей стабилизировалось после сентябрьского всплеска (октябрь: −38%, ноябрь: +3%).
- Количество критичных багов уменьшилось и держится на стабильном уровне (октябрь: −41%, ноябрь: −1%).
- Наблюдается быстрый рост наиболее опасных сценариев эксплуатации (октябрь: +109%, ноябрь: +17%).
- Количество KEV снизилось после сентябрьского пика, но в ноябре злоумышленники вновь активизировались (октябрь: −45%, ноябрь: +17%).

Динамика уязвимостей в Рунете по данным СКИПА: Сентябрь → Октябрь → Ноябрь

	Сентябрь	Октябрь	Ноябрь
Количество уязвимостей	7415	4581 -38%	4742 +3%
High/Critical	3352	1993 -41%	1996 -1%
Уязвимости, просмотренные экспертами	1572	1679 +7%	1748 +4%

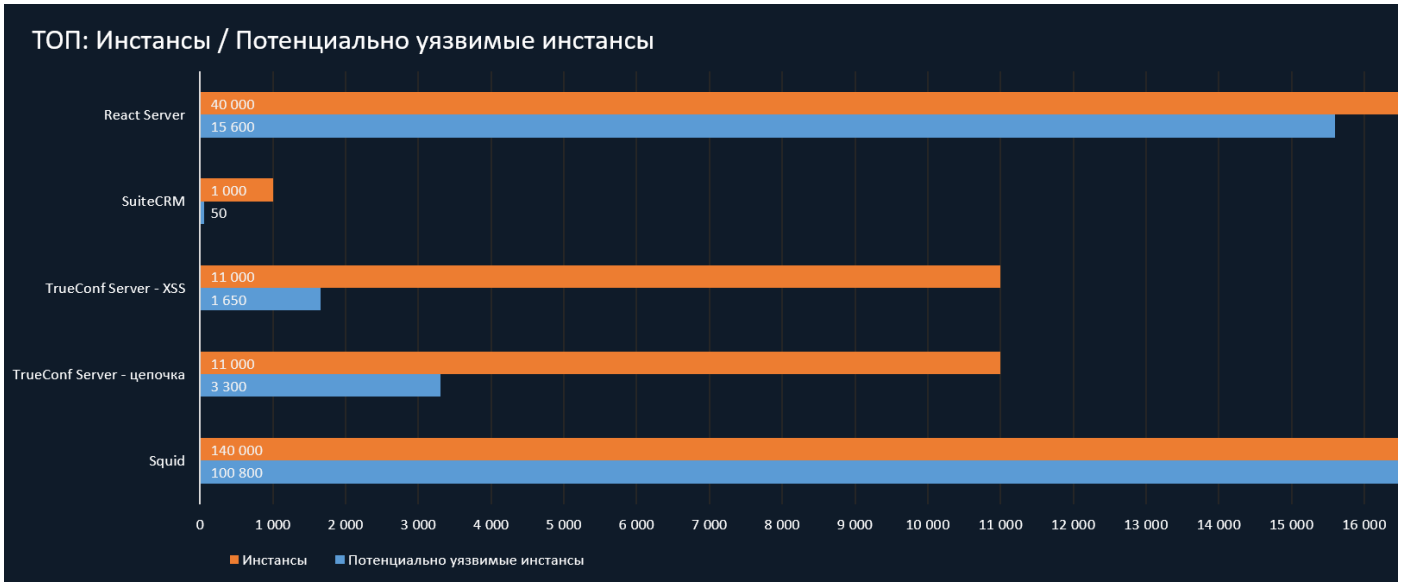
	Сентябрь	Октябрь	Ноябрь
Без привилегий	422	882 +109%	1031 +17%
KEV	84	46 -45%	1996 +17%
Взято в работу	136	139 +2%	195 +40%

Интересно, что по данным зарубежного аналитика Jerry Gamblin, в ноябре 2025 было опубликовано всего 2 900 уязвимостей (а это на 29% меньше, чем в прошлом году!). Однако наша СКИПА зафиксировала 4 742 реальные уязвимости за тот же период. Почему? Разница объясняется тем, что мы используем 15 источников, включая зарубежные CNA, бюллетени вендоров, технические advisories, активные PoC и телеметрию попыток эксплуатации. На самом деле, угроз меньше не стало — просто часть уязвимостей в ноябре не успела получить идентификатор. СКИПА фиксирует такие случаи напрямую - поэтому наш анализ риска остаётся точнее и чувствительнее.

Теперь, когда есть общий фон, посмотрим, какие уязвимости действительно попали в зону риска, а какие просто запугивали без причины.

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. Раскрытие данных в Squid (CVE-2025-62168)

CVSS: 7.5 | KEV: да

Масштаб: На радарах СКИПА мы наблюдаем ~140.000 инстансов Squid, из которых уязвимы около 72%.

Описание: В версиях Squid до 7.2 из-за некорректной обработки ошибок происходило непреднамеренное раскрытие учётных данных, используемых при HTTP-аутентификации. Уязвимость позволяла обходить механизмы защиты и перехватывать токены безопасности или другие чувствительные данные доверенного клиента, в том числе применяемые внутри веб-приложений, использующих Squid для балансировки нагрузки на серверную часть приложения.

Что по факту: Критическое ПО, высокая распространенность в Рунете.

Вердикт: Серьёзная уязвимость, в открытом доступе есть PoC, требуется срочное обновление.

2. SuiteCRM / Кто не экранирует — тот рискует (CVE-2025-64492 / BDU:2025-10914)

CVSS: 8.8 | KEV: нет | COK: да*

Масштаб: На радарах СКИПА мы наблюдаем ~1000 инстансов SuiteCRM, из которых уязвимы около 5% (на момент публикации информации в БДУ)

Описание: В одном из компонентов SuiteCRM была обнаружена уязвимость, связанная с внедрением SQL-кода вслепую по времени. Эта уязвимость позволяет злоумышленнику, прошедшему аутентификацию, получать данные из базы, измеряя время отклика, что потенциально может привести к извлечению конфиденциальной информации.

Что по факту: Публичный PoC отсутствует, доля потенциально подверженных инстансов снизилась примерно до 5%, что демонстрирует слаженную и оперативную работу по управлению уязвимостями.

Вердикт: Риск автоматизированной атаки сильно снижен благодаря оперативному устранению уязвимости и обновлению уязвимых хостов.

**CyberOK Vuln ID (COK) — это внутренний уникальный идентификатор, который исследователи CyberOK присваивают найденным уязвимостям на этапе исследования и до их официальной публикации (например, до присвоения CVE или размещения в бюллетенях поставщика).*

3. TrueConf Server / Что там за кулисами? (BDU:2025-13736 / BDU:2025-13737 / BDU:2025-13738 / BDU:2025-11412)

CVSS: 5.3 - 8.1 | KEV: нет | COK: да

Масштаб: На радарах СКИПА мы наблюдаем ~11.000 инстансов TrueConf, из которых уязвимы около 30% для цепочки и 15% для XSS.

Описание: Цепочка уязвимостей включает обход авторизации, отсутствие ограничений на количество попыток входа и уязвимость, позволяющую выполнять команды операционной системы. Также обнаружена отдельная отражённая XSS-уязвимость, которая может помочь миновать первый и второй этап при автоматизированной эксплуатации.

Что по факту: Публичный PoC отсутствует, уязвимость оперативно устранена, риск автоматизированных атак снижен.

Вердикт: Обновить TrueConf Server до версии 5.5.2. Рекомендуется ограничить доступ к административному интерфейсу, внедрить fail2ban или альтернативные средства защиты серверов от атак методом перебора, настроить WAF/IDS, проверить и сбросить учётные данные администраторов, провести аудит логов и процессов.

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

4. RCE в компонентах React Server / Реактивная паника (CVE-2025-55182)

CVSS: 10.0 | KEV: нет

Мы не смогли проигнорировать факт выхода данной свежей уязвимости и решили включить ее в топ за ноябрь :)

"On November 29th, Lachlan Davidson reported a security vulnerability in React that allows unauthenticated remote code execution by exploiting a flaw in how React decodes payloads sent to React Server Function endpoints."

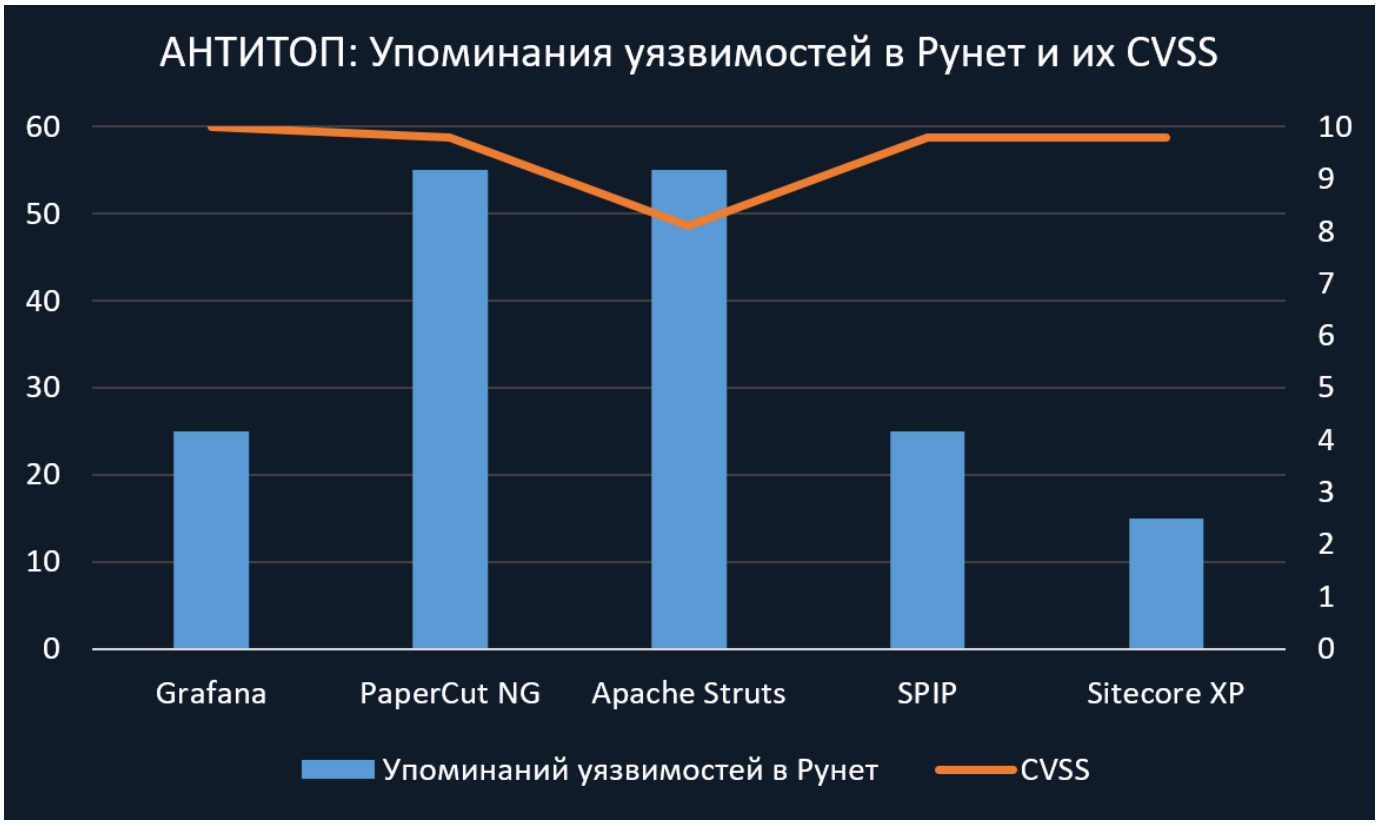
Масштаб: На радарах СКИПА мы наблюдаем более 40.000 инстансов React, которые могут использовать React Server Components, из них уязвимы примерно 40%.

Описание: В компонентах React Server Components версий 19.0.0, 19.1.0, 19.1.1 и 19.2.0, включающих пакеты react-server-dom-parcel, react-server-dom-turbopack и react-server-dom-webpack, обнаружена уязвимость удалённого выполнения кода без предварительной аутентификации. Проблема заключается в небезопасной десериализации полезных данных из HTTP-запросов к конечным точкам функций React Server Components.

Что по факту: Усложнение атак на React связано с тем, что признаки присутствия компонентов на хосте не всегда легко обнаруживаются, что затрудняет их идентификацию. В сети активно обсуждаются PoC и лаборатории для воспроизведения данной уязвимости, единого мнения на этот счет нет, но на данный момент сам автор находки подчеркивает неоднозначность эксплойтов и предупреждает о возможной путанице и ложноположительных результатах.
Предположительно, для успешной атаки требуется знать значение Server Reference ID.

Вердикт: Критическая уязвимость, которая с бешеной скоростью набирает обороты эксплуатации в дикой природе, **патчить незамедлительно**! СКИПА зафиксировала 70+ (!) упоминаний данной уязвимости в сети Интернет.

АНТИТОП: Высокий риск + низкий охват в Рунете



1. Grafana / Укради админки (CVE-2025-41115)

CVSS: 10.0 | KEV: нет | Упоминания СКИПА: 25+

Масштаб: На радарах СКИПА мы наблюдаем ~24.000 инстансов Grafana, из которых уязвимы около 2%.

Описание: При включённом и корректно настроенном SCIM, злоумышленник может отправить специально сформированные запросы к уязвимому инстансу, что позволит захватить учетную запись существующего пользователя вплоть до администратора или создать нового пользователя с высокими привилегиями.

Что по факту: Grafana Cloud и лицензированные облачные провайдеры получили патчи и подтверждают, что их сервисы защищены. Grafana OSS не затронута.

Вердикт: Критическая уязвимость. В момент попадания уязвимости в поле зрения СКИПы, система обнаружила публичный PoC в открытом доступе. Уязвимость легко эксплуатируется на тех инстансах, где остаются токены по умолчанию. Но при этом, массового распространения в Рунете нет, так как требуется специфичная конфигурация Grafana Enterprise и SCIM

2. PaperCut NG / Обход авторизации (CVE-2023-27350)

CVSS: 9.8 | KEV: да | Упоминания СКИПА: 55+

Описание: Уязвимость позволяет удаленным злоумышленникам обходить аутентификацию на уязвимых установках PaperCut NG.

Что по факту: Исторически, СКИПА знает около 11.000 инстансов, но на момент исследования живых хостов не обнаружено.

Вердикт: В Рунете нет живых инстансов.

3. Apache Struts / RCE (CVE-2018-11776)

CVSS: 8.1 | KEV: да | Упоминания СКИПА: 55+

Описание: Apache Struts подвержен удаленному выполнению кода, когда alwaysSelectFullNamespace имеет значение true. Уязвимость возникает в случае, если результаты используются без указания пространства имен, при этом верхний пакет либо не имеет пространства имен, либо использует подстановочные знаки. Аналогичная ситуация наблюдается при использовании тега URL, если для него не заданы значения и действия, а верхний пакет не имеет пространства имен или использует подстановочные знаки.

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

Вердикт: Риск для Рунета минимален.

4. SPIP / RCE (CVE-2023-27372)

CVSS: 9.8 | KEV: нет | Упоминания СКИПА: 25+

Описание: SPIP до версии 4.2.1 допускает удаленное выполнение кода через значения форм в публичной области, поскольку сериализация обрабатывается неправильно.

Что по факту: Есть публичный PoC и публичные nuclei шаблоны.

Вердикт: В русскоязычном сегменте Интернета случаи эксплуатации маловероятны, риск массовых автоматизированных атак низкий.

5. Sitecore XP / RCE (CVE-2021-42237)

CVSS: 9.8 | KEV: да | Упоминания СКИПА: 15+

Описание: В Sitecore XP возможна небезопасная десериализация, позволяющая удалённо выполнять команды на хосте. Эксплуатация не требует аутентификации и специальных настроек.

Что по факту: В ноябре были упоминания данной уязвимости, в сети есть публичный nuclei-шаблон, есть риск автоматизированных атак.

Вердикт: Уязвимость представляет серьёзную угрозу, однако в Рунете крайне мало экземпляров данного ПО, что снижает приоритет для массовых атак. Тем не менее, для уязвимых систем необходимо провести обновление и внедрить защитные меры.

Выводы

Ноябрь вновь показал, что в уязвимостях главное не цифра CVSS, а сочетание массовости ПО и простоты эксплуатации. Именно поэтому в зоне реального риска оказываются Squid и TrueConf — они широко распространены в Рунете, и ошибки в них потенциально приводят к серьёзным инцидентам.

Другие уязвимости звучат грозно на бумаге, но почти не встречаются в российском сегменте, поэтому их реальная опасность существенно ниже. Быстрая реакция вендоров тоже играет роль: пример SuiteCRM показал, как оперативные обновления сокращают долю уязвимых инстансов буквально в считанные дни.

Наш совет: обновлять нужно всё, но первый приоритет отдаём тем сервисам, которые действительно стоят у вас на периметре и имеют подтверждённые векторы эксплуатации. Это и есть реальная кибергигиена.

Мы каждый день копаемся в периметре Рунета и делимся самыми интересными находками. Подписывайтесь на наш телеграм, чтобы не пропустить важное.