4RAYS by SOLAR

ОБЗОР УЯЗВИМОСТЕЙ ВЕБ-ПРИЛОЖЕНИЙ

4-й квартал 2025 года
+ полный 2025 год

Ежедневно эксперты Solar 4RAYS следят за появлением уязвимостей в распространенных веб-приложениях, а также эксплойтов под эти уязвимости. Мониторинг осуществляется для своевременного создания детектирующих логик, которые впоследствии реализуются в продуктах и сервисах «Солара». Параллельно накапливается статистика, которая позволяет понять, как меняется ландшафт угроз этого типа.
В данном отчете мы представляем результаты наших наблюдений за четвертый квартал и по итогам всех 12 месяцев 2025 г. и обзор самых распространенных веб-уязвимостей 2025 года.

Основные результаты: 4-й квартал

В четвертом квартале мы проанализировали 397 сообщений о новых уязвимостях и proof-of-concept для них в более чем 290 продуктах.

- Количество обнаруженных уязвимостей по сравнению с третьим кварталом выросло на 34,1% — с 296 до 397. Это самое большое число обнаруженных уязвимостей по сравнению с предыдущими кварталами года.
- Сетевой вектор имеют 81% уязвимостей, из них в 78,7% используется протокол HTTP. В третьем квартале эти показатели составляли 81,8% и 88% соответственно.
- Средний уровень критичности обнаруженных уязвимостей — 7,8 (такой же был и в третьем квартале).
- Самый уязвимый продукт квартала — WordPress и плагины для него (13,6%). Также второй квартал к ряду выявляются уязвимости в различных AI-сервисах. В топ уязвимых продуктов вошли React, Apache, продукты Fortinet, роутеры и другое сетевое оборудование.
- Большая часть (69,3%) обнаруженных сетевых уязвимостей имели уровень критичности High и Critical. В третьем квартале этот показатель составлял 67,3%.
- Межсайтовый скриптинг, SQL-инъекция, неограниченная загрузка файла опасного типа, внедрение команды ОС, недостаточный контроль генерации кода (внедрение кода), некорректный контроль доступа — наиболее часто обнаруживаемые типы уязвимостей в четвертом квартале 2025 года.

Основные результаты 2025 года

- Всего было проанализировано **более чем 1000 PoC для уязвимостей более чем в 680 продуктах.**
- Самым уязвимым продуктом 2025 года стал WordPress из-за его обширной библиотеки сторонних плагинов и высокой популярности среди других CMS-платформ. **За год было зафиксировано примерно 140 PoC-эксплойтов**.
- Самыми распространенными типами уязвимостей в 2025 году стали: недостаточная нейтрализация ввода при формировании веб-страницы (XSS),

недостаточная нейтрализация специальных элементов в SQL-запросах, межсайтовая подделка запросов (CSRF) и неограниченная загрузка файлов опасного типа.

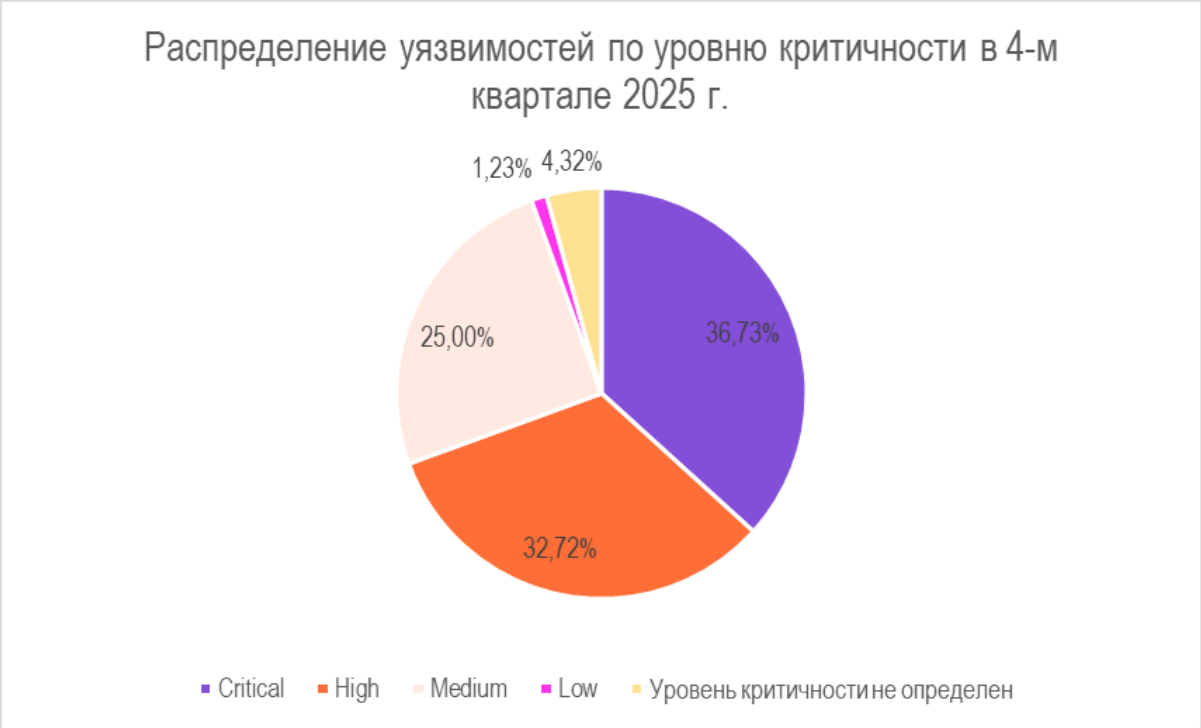
Результаты 4-го квартала

Векторы и уровень критичности

Из всех обнаруженных за квартал уязвимостей сетевой вектор (когда эксплуатация происходит через сетевые протоколы HTTP, SSH, SMB и др.) имеют 81,1%. Из этого объема 78% (255 сообщений об уязвимостях) пришлось на HTTP.

В четвертом квартале мы заметили сообщения о ранее не встречавшемся нам типе — смежных уязвимостях. Это разновидность уязвимостей может быть использована через смежную сеть, то есть атакующий должен быть в той же физической сети или локальной подсети, но не обязательно на самой целевой машине, что указывает на более низкую степень удаленности атаки по сравнению с атаками типа Network (Сеть). Примером такой уязвимости является CVE-2025-67780 — обнаруженная в четвертом квартале брешь в системе спутникового интернета Starlink.

Большая часть (68,4%) обнаруженных сетевых уязвимостей имели уровень критичности High и Critical. Показатель незначительно вырос по сравнению с третьим кварталом, когда на такие уязвимости пришлось 67,3%. Изменение может быть связано с сокращением числа уязвимостей, уровень критичности которых не определен. Под конец года, когда представители всех отраслей, включая исследователей безопасности, стремятся подвести итоги и завершить рабочие задачи, это характерное явление.



Уязвимости в продуктах

WordPress

WordPress до сих пор в ряду первых. За 4-й квартал было опубликовано 44 подтвержденных концепции. Максимальный балл опасности (10/10) получили пять уязвимостей в плагинах для WordPress:
CVE-2025-48148 (StoreKeeper B.V. StoreKeeper) — CWE-434;
CVE-2025-29009 (Webkul Medical Prescription Attachment Plugin) — CWE-434;
CVE-2025-12539 (TNC Toolbox:Web Performance) — CWE-922;
CVE-2025-39401 (WordPress WPAMS Plugin) — CWE-434;
CVE-2025-13390 (Directory Kit) — CWE-303.

CWE — это система нумерации типовых брешей в безопасности продуктов. Вот какие типы уязвимостей приведены выше:

- CWE-434 — уязвимость, позволяющая загружать произвольные файлы. Для WordPress характерна загрузка PHP-shell-файлов.
- CWE-922 — уязвимость, позволяющая получать конфиденциальную информацию, доступы к которой не ограничены должным образом.
- CWE-303 — уязвимость обхода аутентификации.

AI-сервисы

Четвертый квартал показал наличие более серьезных уязвимостей в сервисах, связанных с разработкой AI-ассистентов. Всего стало известно о десяти новых недостатках безопасности. Например:

- *Flowise* — это платформа/инструмент с открытым исходным кодом для создания ИИ-агентов (CVE-2025-59528).

- *Ray* — открытый программный фреймворк (библиотека), в первую очередь для масштабирования задач машинного обучения, обучения моделей и распределенных вычислений (CVE-2025-62593).
  Обе эти уязвимости связаны с удаленным выполнением кода (CWE-94, «инъекция» кода).

- *OpenAI*-Codex CLI — это локальный агент для программирования от OpenAI (CVE-2025-59532). Уязвимость связана в CWE-20 (некорректная проверка входных данных).

React

Самой громкой уязвимостью четвертого квартала можно назвать CVE-2025-55182, которая получила собственное имя React2Shell. О ней мы писали в нашем телеграм-канале. Если кратко, то CVE-2025-55182 позволяла выполнить RCE через «загрязнение» прототипов. Данная уязвимость имеет огромную глубину обфускации, что делает ее еще более опасной. В процессе исследования CVE-2025-55182 также были обнаружены еще две уязвимости: CVE-2025-55184 — угроза DoS и CVE-2025-55183 — угроза раскрытия исходного кода. Об этом мы также писали в нашем канале.

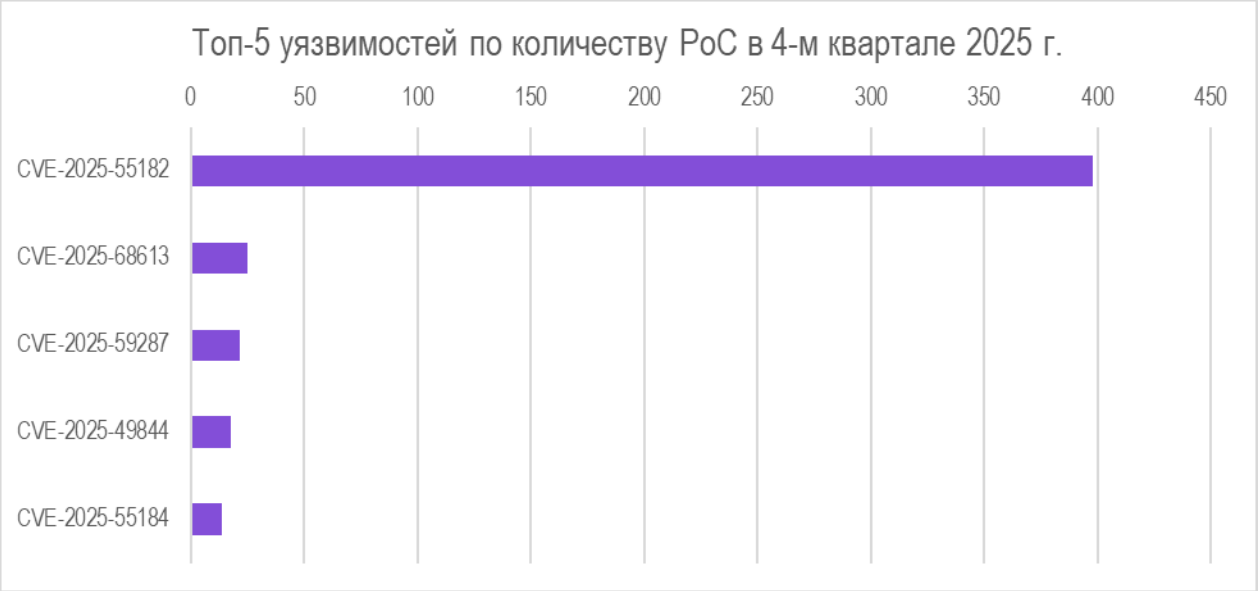
Fortinet

Также стало известно о нескольких критических уязвимостях в продуктах компании Fortinet. Одной из самых известных является CVE-2025-64446 — уязвимость обхода пути, которая может привести к созданию сторонних пользователей с правами администратора. Подробнее о ней читайте в нашем посте.

Apache

Десятибалльная уязвимость в модулях Apache Tika CVE-2025-66516 позволяла внедрять внешние XML-сущности (XXE) с помощью специально созданного XFA-файла внутри PDF-файла.

Топ-5 уязвимостей по количеству вышедших Proof-of-Concept (включая «уязвимость-исключение»)



Некоторые уязвимости, опубликованные в течение квартала, получили несколько реализаций в виде proof-of-concept. Обычно такое происходит с наиболее опасными и/или легко эксплуатируемыми уязвимостями. И как видно из графика выше, React2Shell стал абсолютным чемпионом квартала.

Кратко опишем остальные уязвимости, для которых в исследуемом квартале вышло наибольшее число PoC. Важно отметить, что их количество может меняться со временем.

CVE-2025-68613 (9,9/10): уязвимость выполнения удаленного кода у авторизированных пользователей в n8n. Подробнее можно прочитать в нашем посте.

CVE-2025-59287 (9,9/10): десериализация недостоверных данных в службе обновления Windows Server.

CVE-2025-49844 (9,9/10): уязвимость в СУБД Redis позволяла злоумышленнику выполнять Lua-скрипты. Подробнее — в нашем посте. Данная уязвимость не эксплуатируется через HTTP-протокол, но была включена в рамках офтоп, так как данная СУБД часто использует веб-приложения для хранения различных метрик.

CVE-2025-55184 (7,5/10): уязвимость, позволяющая вызвать отказ в обслуживании в приложениях на React.

CVE-2025-61882 (9,8/10): уязвимость выполнения RCE через обход аутентификации в Oracle E-Business Suite.

На увеличение количества PoC могут влиять публикации или аналитика от

независимых исследовательских подразделений в области кибербезопасности, например: **WatchTowr Labs** и **Arctic Wolf Labs**.

Наиболее часто обнаруживаемые типы уязвимостей

В четвертом квартале мы выделяем 10 типов (приводим их с номерами по Common Weakness Enumeration, CWE) уязвимостей, которые обнаруживаются чаще других.

Уязвимость (CWE)	Количество
CWE-79: Недостаточная нейтрализация ввода при формировании веб-страницы (XSS)	56
CWE-89: Недостаточная нейтрализация специальных элементов в SQL-запросах	22
CWE-434: Неограниченная загрузка файлов опасного типа	19
CWE-94: Недостаточный контроль генерации кода (внедрение кода)	15
CWE-22: Некорректное ограничение доступа	12
CWE-78: Недостаточная нейтрализация специальных элементов в ОС-командах	11
CWE-306: Отсутствие аутентификации для критически важной функции	8
CWE-20: Недостаточная валидация ввода	8
CWE-77: Некорректная нейтрализация специальных элементов, используемых в команде («Внедрение команды»)	7
CWE-200: Раскрытие конфиденциальной информации неуполномоченным лицом	7

CWE-79
Наиболее ярким примером может быть XSS-уязвимость в популярном кросс-платформенном сервере для обмена файлами CrushFTP — CVE-2025-63420.

CWE-89
SQLi-уязвимость в open-source-фреймворке по автоматизации рабочих процессов Melis Platform Framework — CVE-2025-10351.

CWE-434
Об одной из таких уязвимостей мы писали выше. CVE-2025-48148 в плагине для WP (StoreKeeper B.V. StoreKeeper).

CWE-94
Уязвимость в *Flowise* CVE-2025-59528, о которой мы писали выше.

CWE-22
Уязвимость в FortiWeb — CVE-2025-25254.

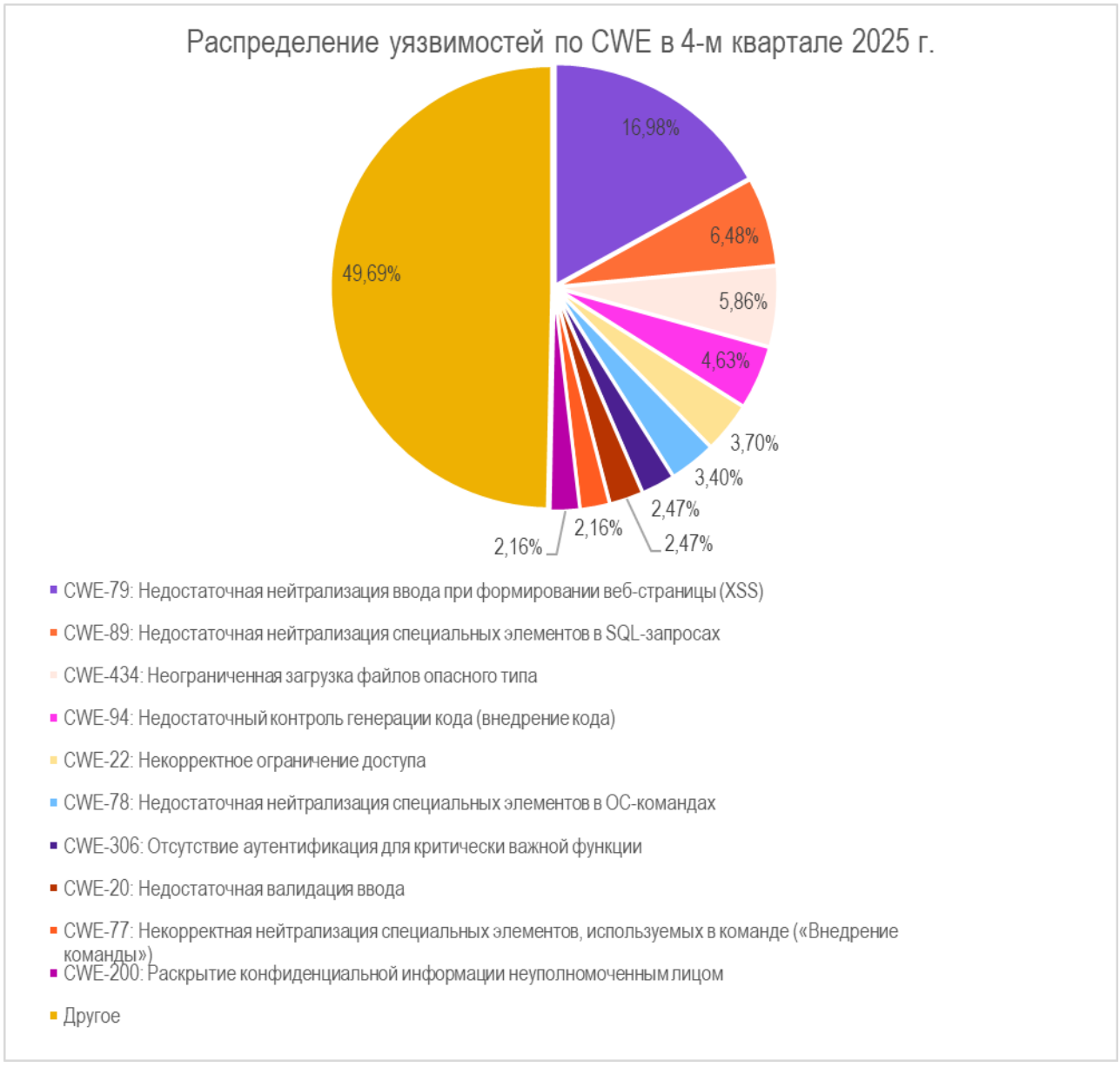
CWE-78
Уязвимость в React Native CLI — CVE-2025-11953.

CWE-306
Уязвимость в Oracle Fusion Middleware — CVE-2025-61757.

CWE-20
Уязвимость в плагине для WP Fox LMS — CVE-2025-14156.

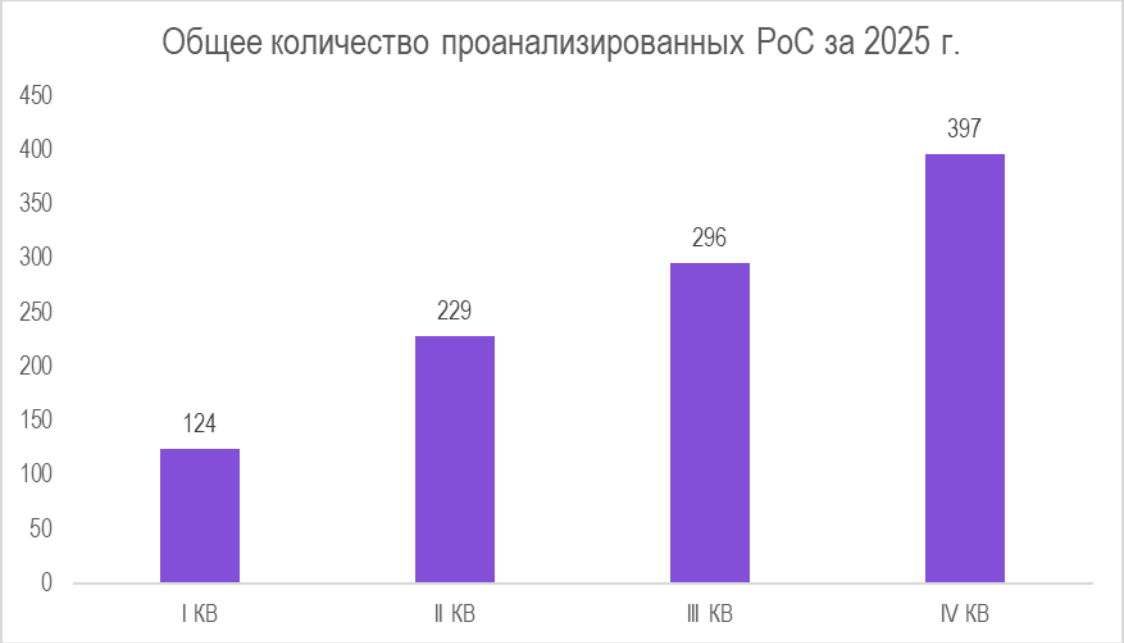
CWE-77
Уязвимость в Zohocorp ManageEngine — CVE-2025-9223.

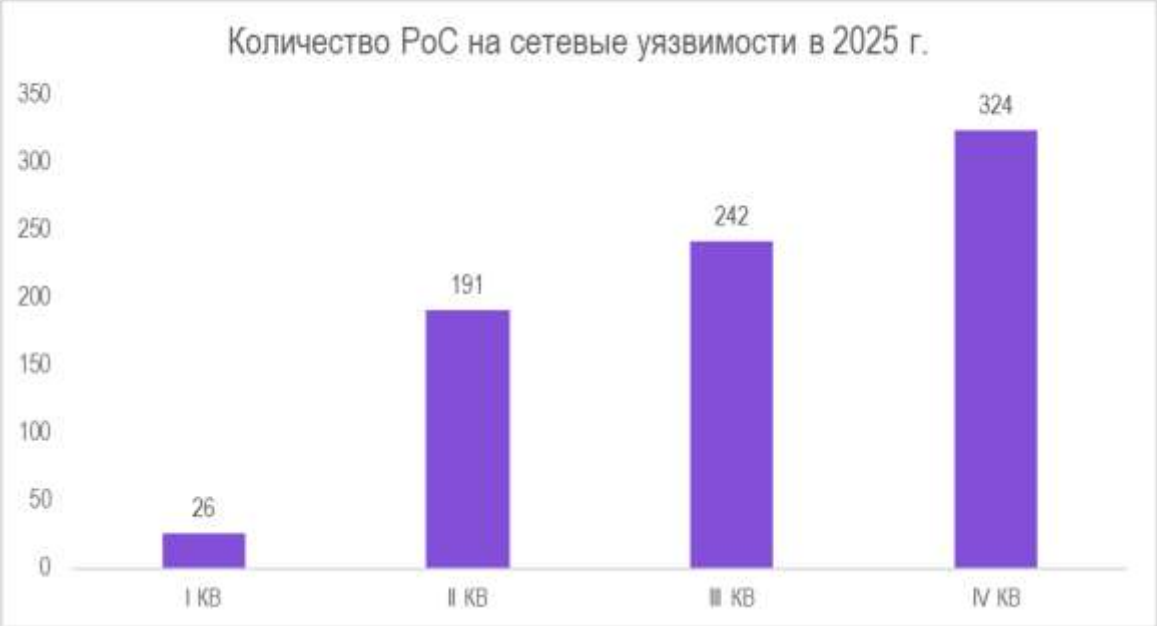
CWE-200
Уязвимость в MikroTik RouterOS — CVE-2025-61481.

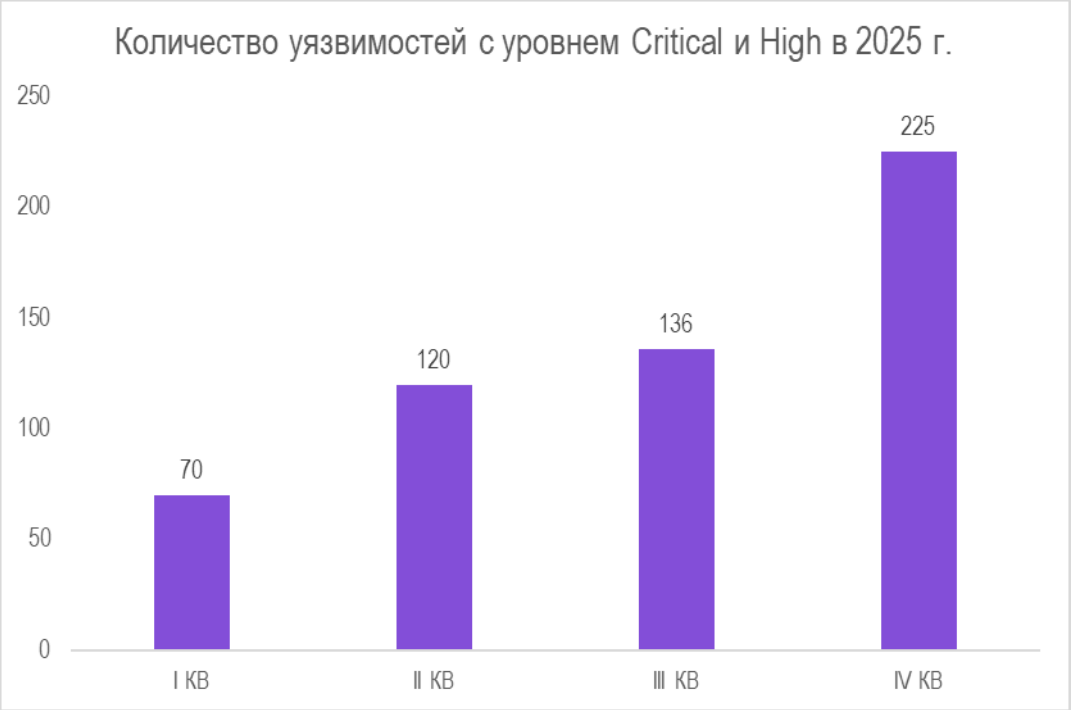


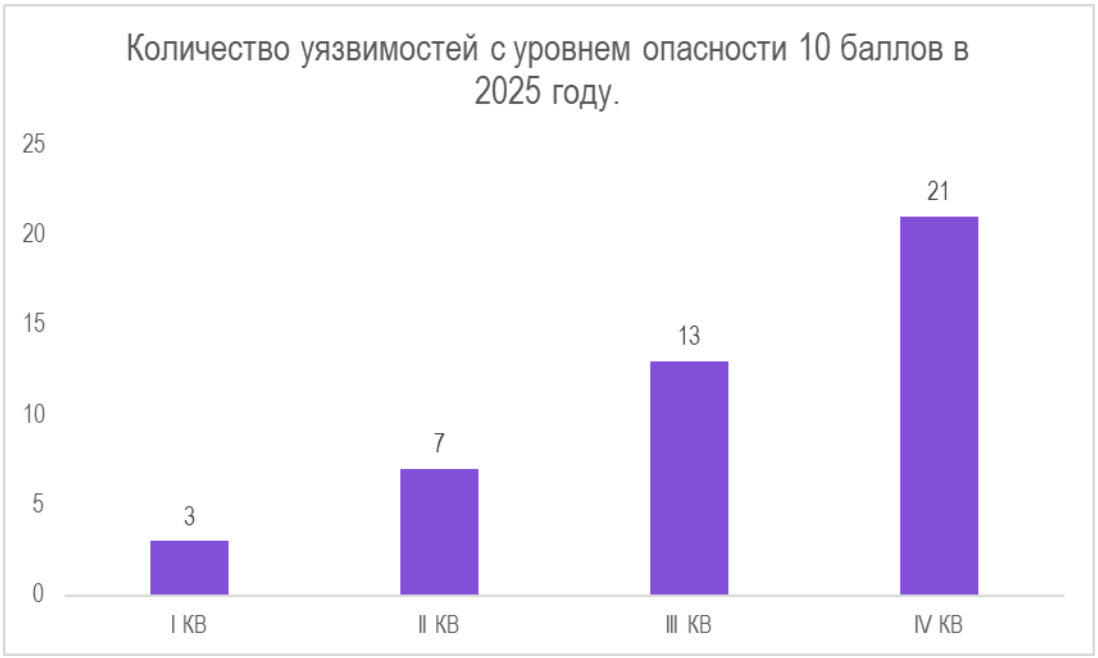
Результаты 2025 года

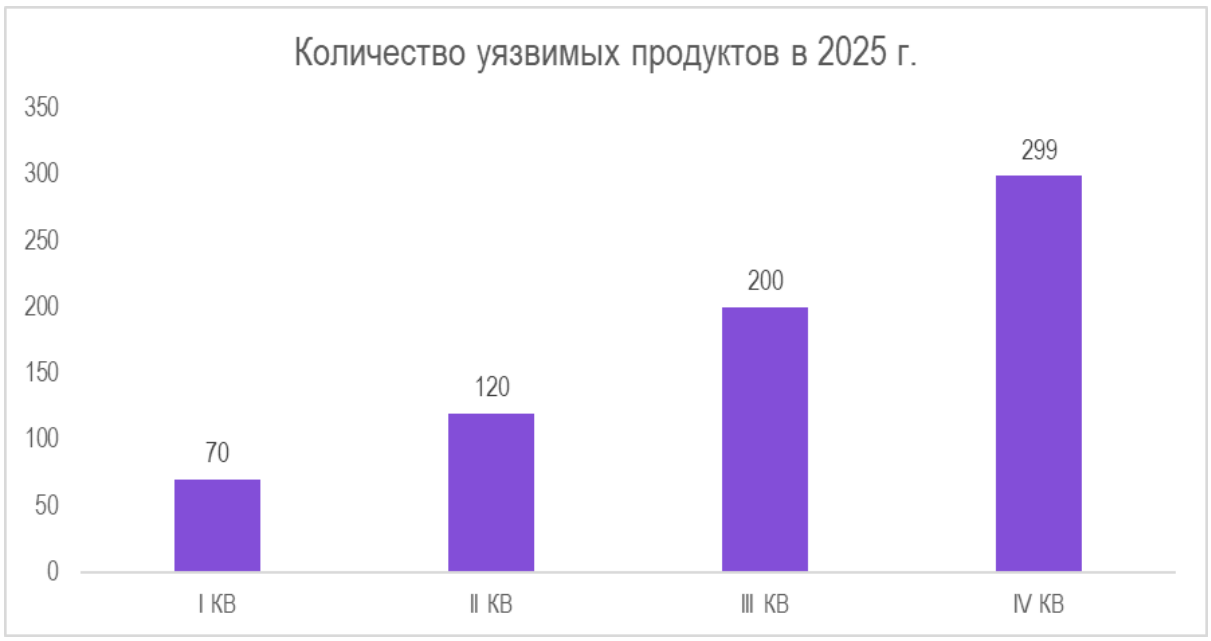
За год было проанализировано 1046 PoC для уязвимостей более чем в 680 продуктах, из которых около 700 эксплуатируются через протокол HTTP. Самым уязвимым продуктом является WordPress из-за его обширной библиотеки сторонних плагинов и высокой популярности среди других CMS-платформ. За год было зафиксировано примерно 140 PoC-эксплойтов. Около 70% всех сетевых уязвимостей имели высокую или критическую степень риска.




Количество PoC на сетевые уязвимости в 2025 г.
350
300
250
200
150
100
50
0
26
191
242
324
I КВ
II КВ
III КВ
IV КВ


Количество уязвимостей с уровнем Critical и High в 2025 г.
250
200
150
100
50
0
70
120
136
225
I КВ
II КВ
III КВ
IV КВ





Представленные графики наглядно демонстрируют последовательное увеличение в течение года числа обнаруженных уязвимостей с критическим приоритетом. При этом отрицательных скачков зафиксировано не было, все показатели только росли. Вторая половина года оказалась самой жаркой в этом смысле порой. Эта тенденция говорит о том, что в ИБ-командам стоит закладывать больше ресурсов на установку обновлений и другие меры по предотвращению атак через эксплойты.

Самые распространенные уязвимости по количеству PoC в течение года

Самая популярная CVE по количеству PoC	
I КВ	CVE-2025-24893
II КВ	CVE-2025-3248
III КВ	CVE-2025-53770
IV КВ	CVE-2025-55182

Итоговая таблица CWE за год

CWE и название
CWE-79 — Недостаточная нейтрализация ввода при формировании веб-страницы (XSS)
CWE-89 — Недостаточная нейтрализация специальных элементов в SQL-запросах (SQL-инъекция)
CWE-434 — Неограниченная загрузка файлов с опасным типом
CWE-94 — Недостаточный контроль генерации кода (внедрение кода)
CWE-22 — Неправильный контроль доступа к путям и файлам (Path Traversal)
CWE-78 — Недостаточная нейтрализация специальных элементов в командах ОС (Command Injection)
CWE-20 — Недостаточная валидация ввода
CWE-284 — Неправильный контроль доступа
CWE-502 — Десериализация ненадёжных данных
CWE-352 — Подделка межсайтовых запросов (CSRF)
CWE-77 — Неправильная нейтрализация специальных элементов в командной строке
CWE-639 — Обход авторизации через управляемый пользователем ключ (IDOR)
CWE-200 — Раскрытие конфиденциальной информации неуполномоченным лицам
CWE-74 — Недостаточная нейтрализация специальных элементов в выводе
CWE-862 — Отсутствие проверки авторизации
CWE-306 — Отсутствует аутентификация для критически важной функции
CWE-918 — Серверный подлог запросов (SSRF)

Можно сказать, что самые типичные уязвимости до сих пор остаются самыми популярными, такие как XSS, SQLi, выход за пределы каталога и т. д.

Заключение

Итоговые данные показывают, что за год количество новых уязвимостей и их PoC только росло. С одной стороны, это свидетельствует об активности сообщества исследователей безопасности продуктов, с другой — о систематических проблемах в некотором ПО. Например, Wordpress оставался самым уязвимым продуктом в течение всего года. Популярные продукты Fortinet, Apache и некоторые другие не раз становились предметом изучения. Зачастую данные исследований в области информационной безопасности приводили к обнаружению серьезных уязвимостей, что еще раз подтверждает: чем популярнее продукт, который вы используете, тем пристальнее нужно следить за его актуальностью.

Одним из ключевых трендов года стало обнаружение уязвимостей в AI-сервисах. Во второй половине года подобные бреши уже дважды входили в топ самого уязвимого популярного ПО. Интерес к теме ИИ-помощников не угасает, новые стартапы в этой области появляются чуть ли не каждый день, но в стремлении быстрее вывести на рынок новый продукт его разработчики не всегда уделяют должное внимание безопасности.

В контексте ИИ пока речь идет об угрозах, связанных с конфиденциальными данными пользователей подобных сервисов, но наступивший 2026-й обещает быть годом активного внедрения в ПО технологий искусственного интеллекта, и в частности ИИ-агентов. Такие продукты не просто обрабатывают пользовательские данные, но могут выполнять конкретные действия от имени пользователя, поэтому эксплуатация уязвимостей в ИИ-агентах чревата гораздо более серьезными последствиям, чем утечка данных.

Предполагаем, что в 2026 году исследователи в области информационной безопасности (а вместе с ними и злоумышленники) не оставят без внимания и подобные продукты, и своих «обычных подозреваемых» вроде CMS, серверных решений, роутеров и сетевого оборудования и прочих корпоративных ПО.

В связи с этим Solar 4RAYS советует пристально следить за информацией о новых уязвимостях и своевременно устанавливать обновления для обеспечения безопасности.

О самых опасных уязвимостях мы оперативно пишем посты с рекомендациями в нашем телеграм-канале. Подписывайтесь и будьте в курсе новостей!

Приложение

Посты об опасных уязвимостях в телеграм-канале «Четыре луча», выпущенные за год.

I КВ
CVE-2025-30208
IngressNightmare
CVE-2025–29927
CVE-2025-24893
CVE-2025-24016

II КВ

CVE-2025-32375
API to SSTI to RCE на примере @fastify/view
CVE-2025-48827
CVE-2025-27817
CVE-2025-31125
CVE-2025-3248
CVE-2025-32433
CVE-2025–39601

III КВ

CVE-2025-47812
CVE-2025-53770
CVE-2025-5777
CVE-2025-53833
CVE-2025–50460
CVE-2025-8723
CVE-2025–34159
CVE-2025-58443
CVE-2025-49533
CVE-2025-59934

IV КВ
CVE-2025-49844
CVE-2025-58434
CVE 2025–20282
CVE-2025-62168
CVE-2025-11953
CVE-2025-12907
CVE-2025-64446
CVE-2025-41115
CVE-2025-55182
CVE-2025-55184 и CVE-2025–55183

CVE-2025-68613