4RAYS by SOLAR

ОБЗОР УЯЗВИМОСТЕЙ ВЕБ-ПРИЛОЖЕНИЙ

Отчет по итогам
3-го квартала 2025 года

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 сформировать представление об изменениях в ландшафте угроз этого типа.

В третьем квартале мы проанализировали 296 сообщений о новых уязвимостях и proof-of-concept для них в более чем 200 продуктах. В этой статье расскажем о результатах нашего анализа.

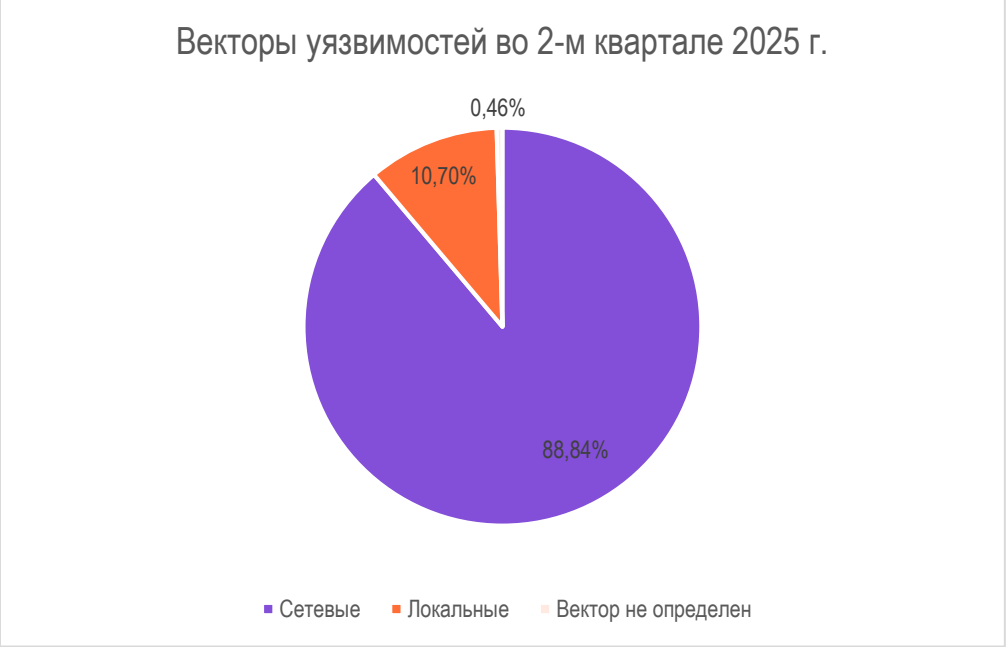
Основные результаты:

- Количество обнаруженных уязвимостей по сравнению со вторым кварталом выросло на 37,7% — с 215 до 296.
- Сетевой вектор имеют 81,8% из них, в 88% используется протокол HTTP.
- Средний уровень критичности обнаруженных уязвимостей — 7,8.
- Самый уязвимый продукт квартала — Wordpress и плагины для него (9%). Также обнаружены уязвимости в AI-сервисах, библиотеках Node.js, продуктах Fortinet, в различных роутерах и другом сетевом оборудовании.
- Большая часть (67,3%) обнаруженных сетевых уязвимостей имела уровень критичности High и Critical.
- Межсайтовый скриптинг, SQL-инъекция, неограниченная загрузка файла опасного типа, внедрение команды ОС, обход авторизации с помощью ключа, контролируемого пользователем, — наиболее часто обнаруживаемые типы уязвимостей в третьем квартале.

Векторы и уровень критичности

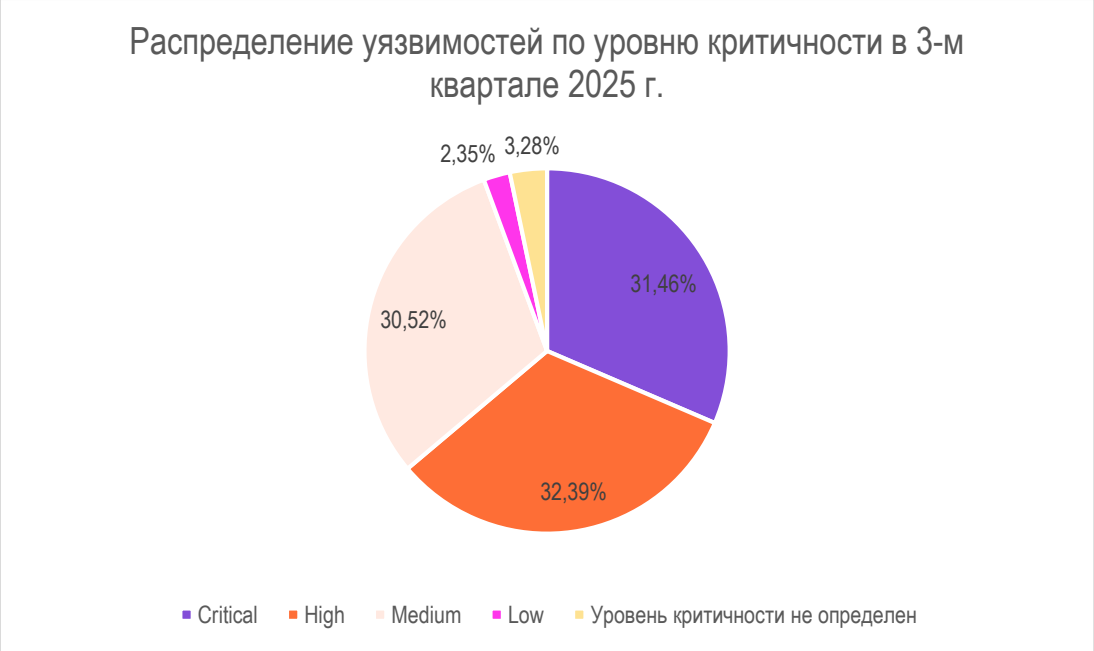
Из всех обнаруженных за квартал уязвимостей сетевой вектор (когда эксплуатация происходит через сетевые протоколы HTTP, SSH, SMB и др.) имеют 81,8%. Из этого объема 88% (213 сообщений об уязвимостях) пришлось на HTTP.

По сравнению со вторым кварталом доля сетевых уязвимостей упала на 9 процентных пунктов (п. п.). Падение обусловлено ростом количества уязвимостей, имеющих локальный характер.

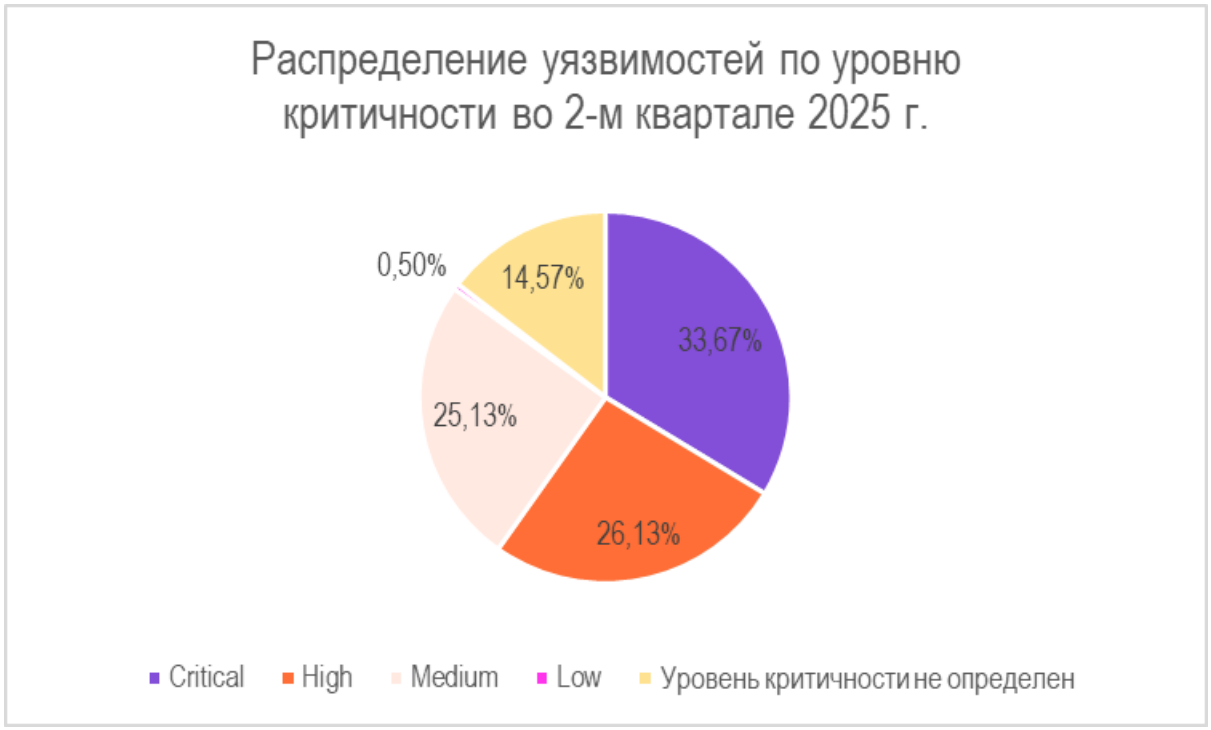


Значительный рост совокупного количества уязвимостей обусловлен сезонным фактором.

Большая часть (67,3%) обнаруженных сетевых уязвимостей имела уровень критичности High и Critical. В предыдущем квартале на такие уязвимости пришлось 59,7%.



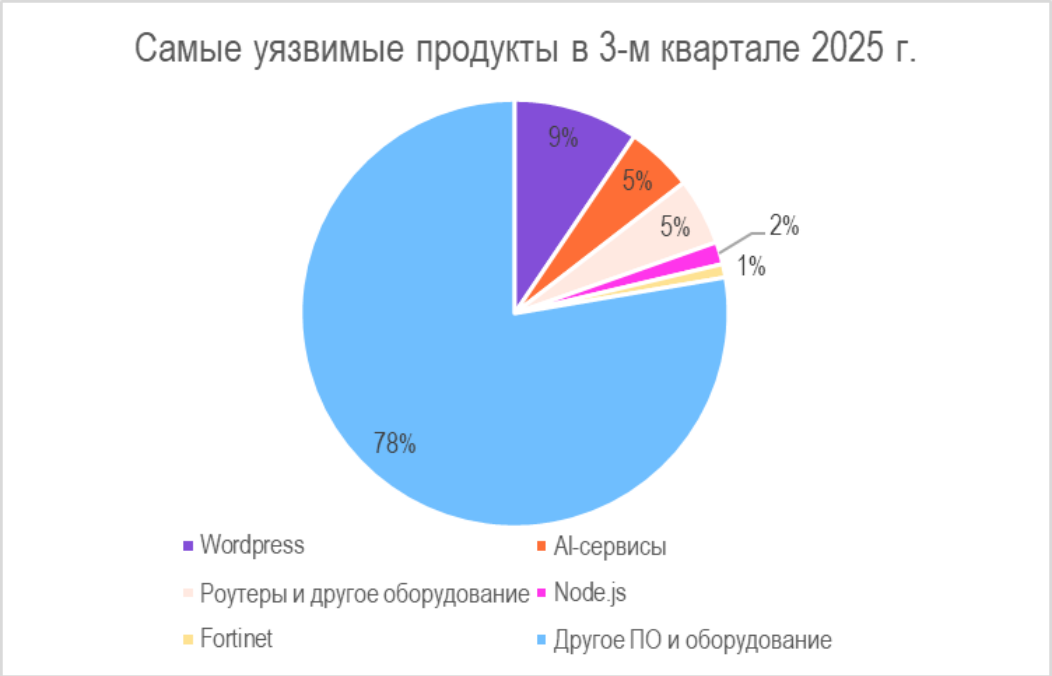
Важно отметить, что в 3-м квартале доля High-уязвимостей выросла на 7,8 п. п. и стала практически равной Critical. Данное изменение может быть обусловлено тем, что общая доля not-defined-уязвимостей сократилась практически на 23 п. п. — то есть сообщения об уязвимостях в третьем квартале обрабатывались оперативнее и им быстрее присваивалась степень критичности.


Распределение уязвимостей по уровню критичности во 2-м квартале 2025 г.
0,50%
14,57%
33,67%
25,13%
26,13%
Critical
High
Medium
Low
Уровень критичности не определен

Уязвимости в продуктах

Wordpress

Лидерство по количеству опубликованных PoC третий квартал подряд занимает CMS-платформа с открытым кодом Wordpress. За 3-й квартал было опубликовано 28 сообщений. Максимальный балл критичности (10/10) получили две уязвимости в плагинах Pie Register plugin (CVE-2025-34077) и Simple File List plugin (CVE-2020-36847). CVE-2025-34077 — позволяет обойти аутентификацию, CVE-2020-36847 — выполнить RCE путем переименования файла png в php.



В третьем квартале доля уязвимостей, связанных с **WordPress**, сократилась на **53,85%** относительно предыдущего квартала. Это частично объясняется тем, что ряд опубликованных ранее PoC позже был удален из открытого доступа, а также тем, что некоторые CVE оказались дубликатами уже известных проблем. Даже с учетом этих факторов WordPress остается лидером по количеству уязвимостей, поэтому при использовании этой CMS следует особенно внимательно следить за актуальностью устанавливаемых плагинов.

AI-сервисы

За третий квартал было опубликовано 15 PoC-уязвимостей в различных AI-сервисах (Aibox, Liner, Telegai, Deepy, Chaindesk). Ранее столь активного появления уязвимостей под такие платформы мы не наблюдали, этот всплеск происходит впервые. Примером такой уязвимости является CVE-2025-51865 (8,8, High), позволяющая злоумышленникам получать конфиденциальную информацию путем перечисления ключей потоков в URL-адресе (IDOR) в веб-сервисе Ai2 Playground. Большая часть уязвимостей, найденных в AI-сервисах, связана с XSS (CWE-79) и IDOR (CWE-639).

Все это не слишком сложные уязвимости, связанные не столько с какими-то специфическими особенностями работы самих AI-сервисов, сколько с тем, что многие из них находятся на стадии стартапов и команды разработки пока еще не уделили достаточно внимания даже базовой безопасности своих сетевых ресурсов. Судя по количеству опубликованных PoCs, исследователи безопасности (а значит, и злоумышленники) всерьез заинтересовались данными сервисами, и их разработчикам самое время вплотную заняться хотя бы базовой безопасностью. В противном случае вероятны крупные инциденты, связанные с утечками пользовательских данных и работоспособностью самих сервисов.

Node.js

Библиотеки и фреймворки для Node.js также стали предметом исследований в третьем квартале. Так, например, уязвимость CVE-2025-7783 получила рейтинг критичности 9,4. CVE-2025-7783 — уязвимость использования недостаточно случайных значений в form-data допускает загрязнение параметров HTTP.

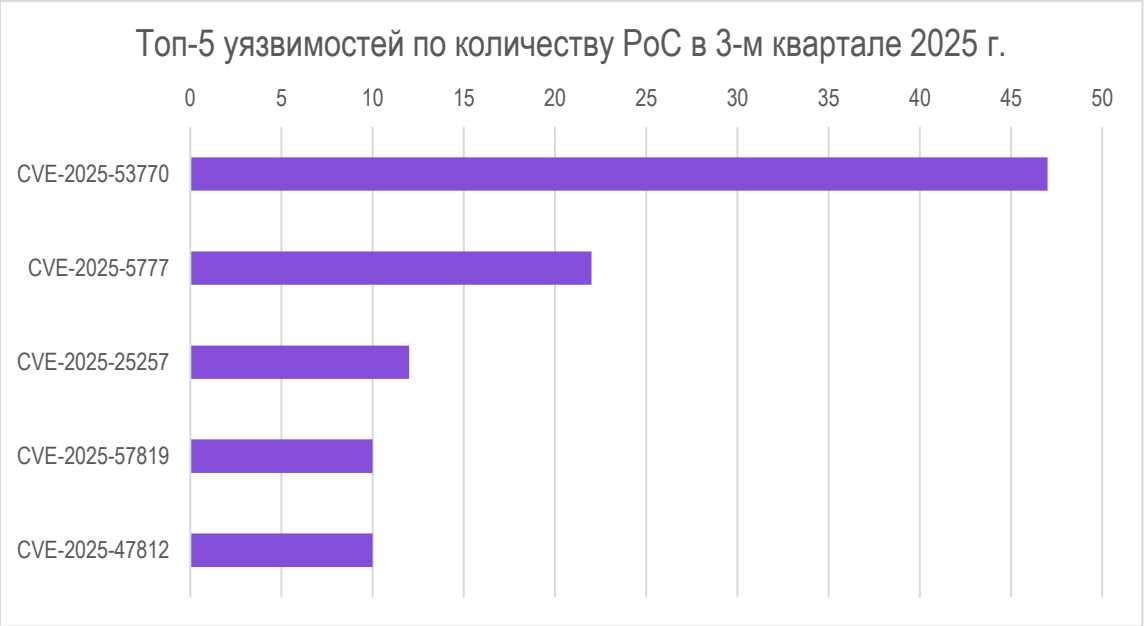
Fortinet

Стало известно минимум о трех PoC-эксплойтах в продуктах Fortinet, опубликованных в публичном доступе. Например, CVE-2025-25257 (9,8 CRITICAL) — уязвимость в Fortinet FortiWeb, позволяющая внедрять команды SQL.

Citrix

Также стало известно о минимум трех публичных PoC-эксплойтах в продуктах Citrix. Об уязвимости в NetScaler ADC and Gateway мы писали в нашем блоге (CVE-2025-5777).

Топ-5 уязвимостей по количеству вышедших Proof-of-Concept



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. Кратко опишем уязвимости, для которых в прошедшем квартале вышло наибольшее число PoC.

CVE-2025-53770 (9,8/10), также известная как ToolShell. Десериализация ненадежных данных в локальном Microsoft SharePoint Server позволяет неавторизованному злоумышленнику выполнить код по сети. Данная уязвимость является, пожалуй, самой громкой за весь третий квартал. Мы писали о ней у нас в блоге.

CVE-2025-5777 (9,3/10) — уязвимость в Citrix NetScaler ADC and Gateway. О которой мы говорили выше.

CVE-2025-25257 (9,8/10) — уязвимость в Fortinet FortiWeb, которую мы также упоминали выше.

CVE-2025-57819 (10/10) — уязвимость в *FreePBX* (модуль **endpoint**), при которой ненадежная обработка входных данных позволяет **обойти аутентификацию** и выполнить **неаутентифицированную SQL-инъекцию**, приводящую к **удаленному выполнению кода (RCE).**

CVE-2025-47812 (10/10) — уязвимость **удаленного выполнения кода (RCE)** в **Wing FTP Server** (версии до 7.4.4). Подробнее об уязвимости читайте в нашем телеграм-канале (https://t.me/four_rays/112).

На рост количества PoC могут влиять публикации или работы независимых исследовательских подразделений в области кибербезопасности, например: **WatchTowr Labs** и **Arctic Wolf Labs**.

Наиболее часто обнаруживаемые типы уязвимостей

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

Уязвимость (CWE)	Количество в 3-м квартале	Количество во 2-м квартале	Изменение
CWE-79: недостаточная нейтрализация ввода при формировании веб-страницы (XSS)	43	26	+65.38%
CWE-89: внедрение SQL-кода (SQL-инъекция)	35	10	+250%
CWE-434: неограниченная загрузка файлов опасного типа	14	23	−64.29%
CWE-78: недостаточная нейтрализация специальных элементов в ОС-командах	14	–	–
CWE-639: обход авторизации через управляемый пользователем ключ (IDOR)	13	–	–
CWE-502: десериализация ненадежных данных	12	5	+140%
CWE-94: недостаточный контроль генерации кода (внедрение кода)	11	10	+10%
CWE-74: недостаточная нейтрализация специальных элементов в выводе	11	–	

CWE-20: недостаточная валидация ввода	10	–	
CWE-77: недостаточная нейтрализация специальных элементов в командах (внедрение кода)	8	–	

Первое место, как и в прошлом квартале, заняли уязвимости межсайтового скриптинга (XSS). Характерным примером такой уязвимости в 3-м квартале была CVE-2025-44136 с критичностью 9,6/10 в продукте MapTiler Tileserver-php v2.0.

Второе место заняли уязвимости внедрения SQL-кода. Ярким примером является описанная выше CVE-2025-57819.

Третье и **четвертое место** заняли уязвимости неограниченной загрузки файлов опасного типа, например описанная выше CVE-2020-36847, и внедрение команд ОС, например CVE-2025-34030.

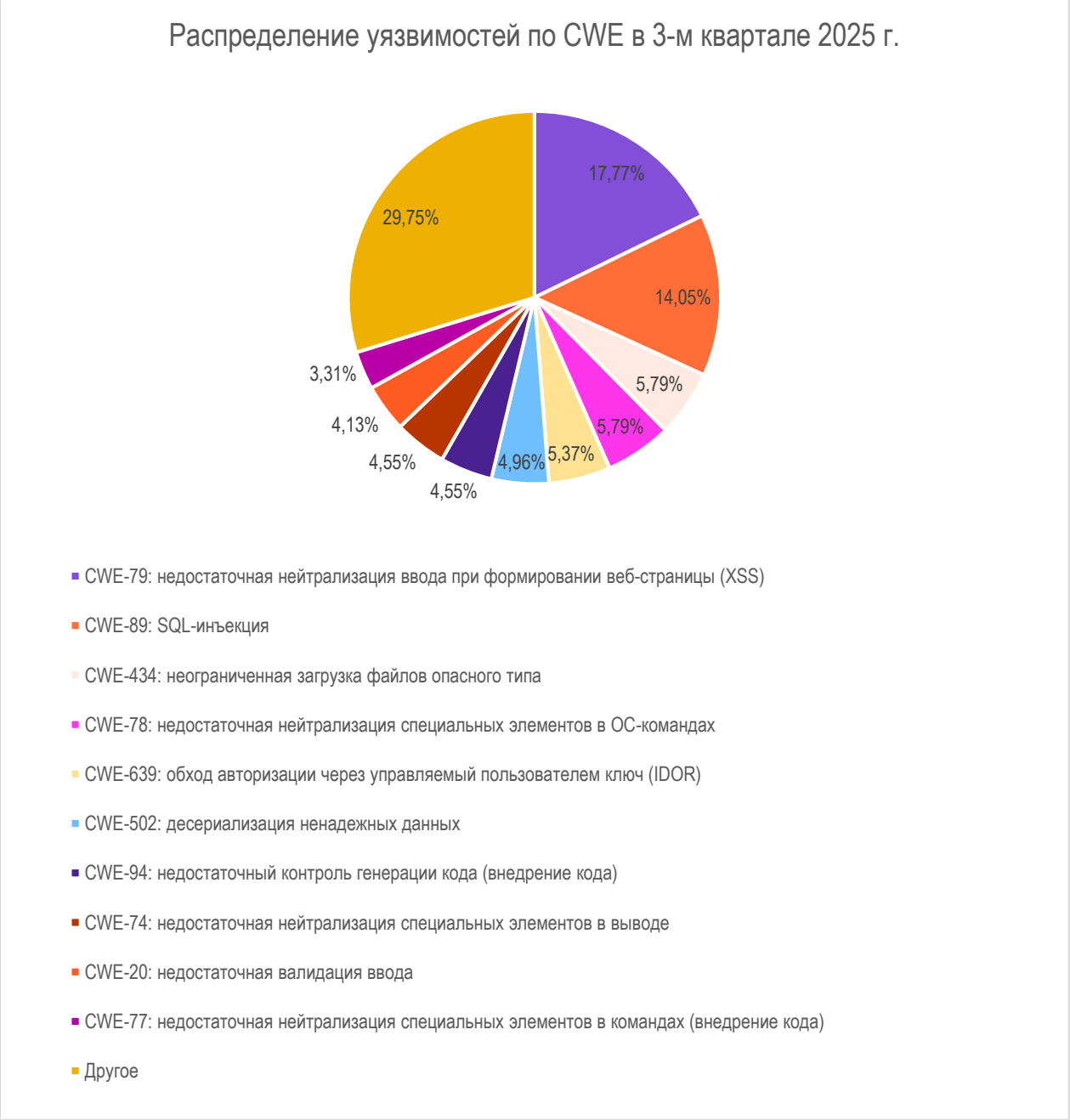
Пятое место заняли IDOR-уязвимости, например описанная выше CVE-2025-51865.

Шестое место заняли уязвимости десериализации ненадежных данных. Например, CVE-2025–50460, о которой мы выпускали лабораторную работу в нашем телеграм-канале (https://t.me/four_rays/121).

Седьмое и **восьмое место заняли** уязвимости внедрения кода и недостаточная нейтрализация специальных элементов в выводе. Для уязвимости внедрения кода характерным примером является CVE-2025–34161, о которой мы упоминали в нашем канале. Недостаточная нейтрализация специальных элементов в выводе часто является вспомогательной уязвимостью к другим типам уязвимостей.

Девятое место заняла уязвимость недостаточной валидация ввода, которая, в свою очередь, также часто является вспомогательной.

Десятое место заняли уязвимости недостаточной нейтрализации специальных элементов в командах. Например, CVE-2025-54782.



В третьем квартале в рейтинг вошла уязвимость **IDOR**. Во-первых, этому риску подвержены многие AI-сервисы. Кроме того, на фоне роста числа **SQL-уязвимостей** увеличилось и количество случаев, связанных с **недостаточной нейтрализацией специальных элементов в выводе**, поскольку она часто выступает вспомогательным фактором при эксплуатации. Аналогичную ситуацию можно наблюдать и с уязвимостью **недостаточной валидации ввода**, которая нередко сопровождает атаки **XSS**. Также в рейтинг попали две уязвимости, позволяющие внедрять код CWE-77 и CWE-94. Чтобы не запутаться, кратко изложим их отличия.

CWE-77 — Command Injection

Позволяет злоумышленнику вставить и выполнить **команды оболочки ОС** через уязвимый вызов (например, os.system('ping ' + user_input)). В результате атакующий может изменить командную строку и заставить приложение выполнить дополнительные или другие системные команды.

CWE-94 — Code Injection

Позволяет злоумышленнику вставить и выполнить **произвольный программный код** внутри интерпретатора приложения (например, eval(user_input) в PHP/Python/JS). Атакующий получает возможность вызвать функции и выполнить логические операции в контексте приложения.

Заключение: обновляйтесь

Общую ситуацию на ландшафте угроз в третьем квартале 2025 года можно охарактеризовать так: стабильный рост выводимых PoC и громкий всплеск ToolShell, **Citrix и Fortinet.**

Еще один скачок третьего квартала — уязвимости, связанные с AI-сервисами. И если вы их разрабатываете или защищаете, убедитесь, что ваши тылы прикрыты и патчи установлены. Предполагаем, что в дальнейшем уязвимости AI-платформ будут нашей обыденностью.

Вывод всегда может быть только один, следите за обновлениями ПО и своевременно обновляйтесь**.**

Также рекомендуем обратить внимание на уязвимости в ПО, о которых мы писали в нашем телеграм-канале:

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

В канале мы пишем только о самых опасных или массовых уязвимостях, которые требуют оперативной реакции. Словом, обновляйтесь.

Команда Solar 4RAYS продолжит наблюдать за ландшафтом и публиковать обновления в блоге.