4RAYS by SOLAR

ОБЗОР СЕТЕВЫХ УЯЗВИМОСТЕЙ

2 квартал 2026 года

Ежедневно эксперты Solar 4RAYS следят за появлением новых уязвимостей и эксплойтов. Мониторинг осуществляется для своевременного создания детектирующих логик, которые впоследствии реализуются в продуктах и сервисах «Солара». Параллельно накапливается статистика, которая позволяет сформировать представление об изменениях на ландшафте угроз этого типа. В данном отчете мы представляем результаты мониторинга об обнаруженных сетевых уязвимостях во втором квартале 2026 года.

Ключевые выводы

- Количество обнаруженных уязвимостей во втором квартале 2026 года по сравнению с первым кварталом 2026 года выросло на 59,8%: с 426 до 681. Такой рост обусловлен как сезонным фактором, так и тем, что второй квартал принес большое количество уязвимостей в Linux и Windows.

- Сетевой вектор имели 83,84% обнаруженных уязвимостей, как и в первом квартале 2026 года.

- Средний уровень критичности обнаруженных сетевых уязвимостей составил 7,9 балла. В первом квартале — 8,1.

- 90,2% всех обнаруженных сетевых уязвимостей эксплуатируются через HTTP. Ближайший «преследователь» — TCP (1,23%)

- Сетевые уязвимости уровня Critical и High в совокупности занимают 73,5% от общей массы всех сетевых уязвимостей. В первом квартале этот показатель составлял 72,06%.

- Уязвимости плагинов и тем для CMS WordPress составили 17,9%. Доля таких уязвимостей в общем объеме упала на два процентных пункта в сравнении с первым кварталом.

- На ИИ-сервисы пришлось 4,83% всех сетевых уязвимостей. Средняя критичность 8.

Краткая справка

Общая статистика по всем сетевым уязвимостям

Во втором квартале мы проанализировали 681 сообщений о новых уязвимостях и proof-of-concept (PoC). Количество сетевых уязвимостей составило 571. Анализировались не только уязвимости 2026 года, но и бреши, обнаруженные в 2025-

м, но опубликованные в этом году. В статистике отражены 89 «прошлогодних» уязвимостей.

В этом отчете расскажем о результатах нашего анализа сетевых уязвимостей — еще раз отметим, что все описанные ниже уязвимости имеют подтверждение, а значит, могут представлять реальную опасность.

В первой части отчета мы опишем уязвимости, не связанные с протоколом HTTP, и отдельно о нем поговорим во второй части отчета, так как данный протокол является доминирующим протоколом доставки полезной нагрузки.

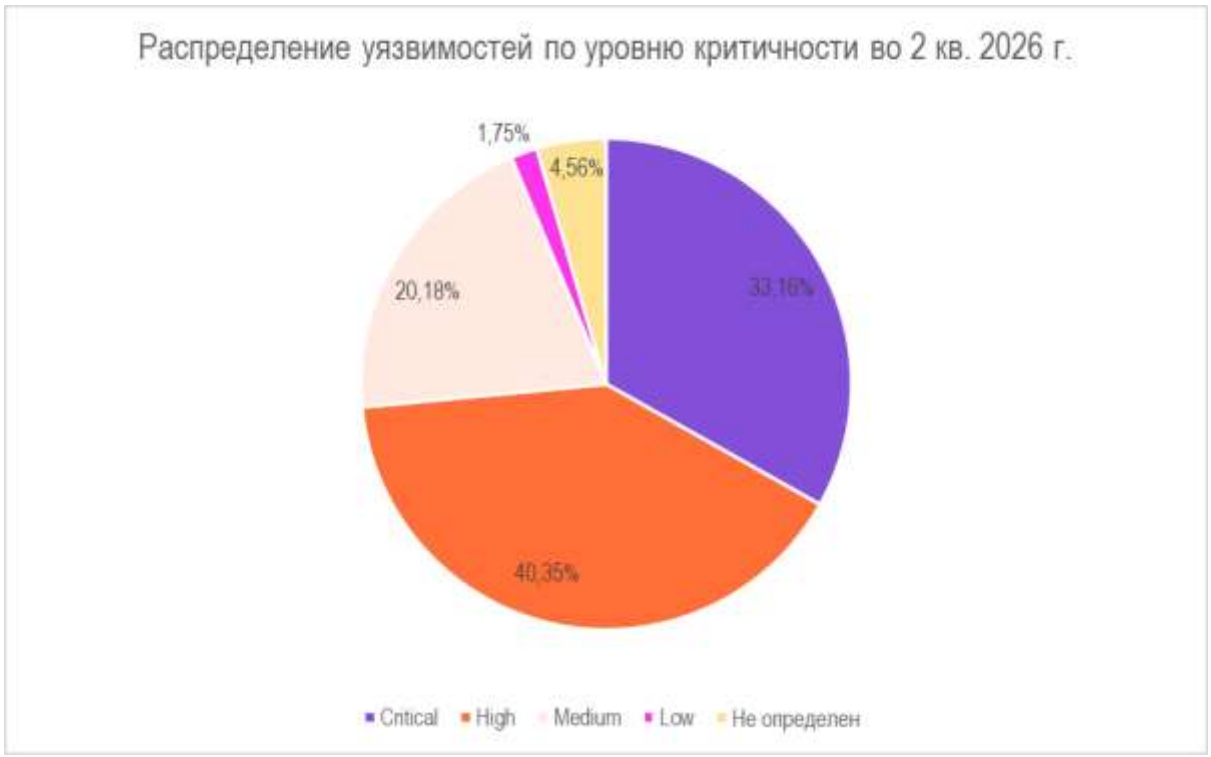
Распределение векторов эксплуатации по сетевым протоколам, а также каналам и средам передачи данных:

Протокол	**Count**	**%**
HTTP	515	90,19
TCP	7	1,23
HTTP2/HTTP3	6	1,05
DNS	5	0,88
SSH	5	0,88
FTP	4	0,70
UDP	4	0,70
WebSocket	4	0,70
gRPC	3	0,53
SMB	3	0,53
Другие	15	2,63

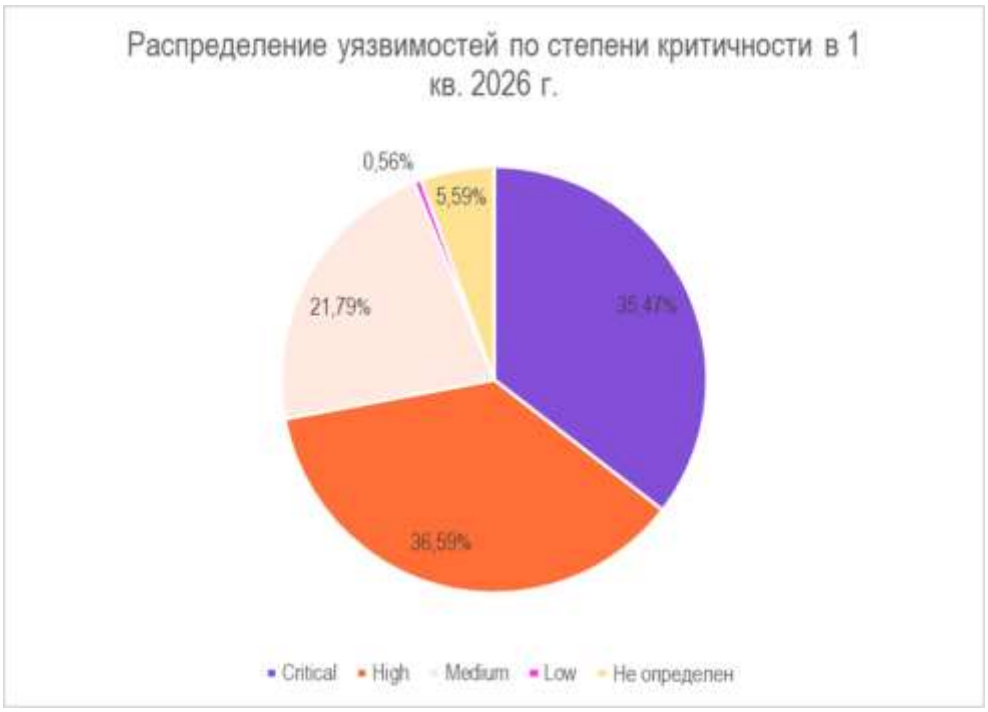
Следует отметить, что немалая часть сетевых уязвимостей не имеет определенного протокола передачи, поскольку полезная нагрузка может быть доставлена различными способами. Это характерно, в частности, для уязвимостей в библиотеках, компонентах обработки входных данных, сетевых стеках и серверных модулях, где способ эксплуатации зависит от конкретного приложения или конфигурации уязвимого

компонента. В таких случаях указание одного конкретного протокола может исказить оценку поверхности атаки.

Распределение критичности уязвимостей, включая сетевой вектор:



В первом квартале распределение было похожим:



Как видно, доля уязвимостей с критическим уровнем немного сократилась, а уязвимости с высоким уровнем выросли почти на четыре процентных пункта.

Распределение уязвимостей по степени критичности (количество) в 2 кв. 2026 г.				
Critical	High	Medium	Low	Не определен
189	230	115	10	26
Распределение уязвимостей по степени критичности (количество) в 1 кв. 2026 г.				
Critical	High	Medium	Low	Не определен
127	131	78	2	20
Рост				
48,82%	75,57%	47,44%	400%	30%

Уровни критичности (баллы)	кв. 2	кв. 1
Максимальный	10	10
Минимальный	2,0	2,3
Средний	7,9	8,1

Сетевые уязвимости, не связанные с протоколом HTTP, Websocket и gRPC

В данную категорию уязвимостей мы отнесли все уязвимости, которые могут эксплуатироваться злоумышленниками как из внешней, так и из внутренней сети по протоколам TCP, DNS, SSH, FTP, UDP, SMB, DHCP и другим, за исключением HTTP, Websocket и gRPC.

Общее число таких уязвимостей составило 75. Средняя критичность — 7,9 по шкале CVSS. Лидирующими CWE стали: CWE:122 — Heap-based Buffer Overflow и CWE-78 —

OS Command Injection. Наиболее уязвимыми оказались продукты Apache: Camel, MINA’s, Tomcat, Arflow, — за ними следует сервер dnsmasq.

Распределение уязвимостей по присвоенному CWE:

Значение	Количество	Доля от CVE, %
CWE-78	8	10,67%
CWE-122	7	9,33%
CWE-77	5	6,67%
CWE-416	3	4,00%
CWE-502	3	4,00%
CWE-94	3	4,00%
CWE-119	2	2,67%
CWE-121	2	2,67%
CWE-200	2	2,67%
CWE-287	2	2,67%
CWE-89	2	2,67%
CWE-943	2	2,67%
Другие	26	34,67%
Не указано	8	10,64%

Уязвимости, которые привлекли наше внимание:

CVE-2026-34159 (9,8/10) — критическая уязвимость в llama.cpp, позволяет запускать языковые ИИ-модели локально. Удаленный неаутентифицированный атакующий, имеющий TCP-доступ к RPC-порту сервера, может читать и записывать память процесса. Совместно с утечкой адресов через RPC-операции выделения буферов это позволяет обойти ASLR и выполнить произвольный код на сервере.

CVE-2026-33453 (10/10) — десятибалльная уязвимость в компоненте camel-coap фреймворка Apache Camel. Компонент принимает параметры из CoAP-запроса и без достаточной фильтрации превращает их во внутренние заголовки Camel. Более подробно об этой уязвимости мы писали здесь.

CVE-2026-40473 (8,8/10) и CVE-2026-40858 (8,8/10) — две уязвимости небезопасной десериализации в различных компонентах Apache Camel, которые в определенных конфигурациях могут привести к удаленному выполнению кода.

CVE-2026-42779 (9,8/10) — критическая уязвимость десериализации в Apache MINA. В затронутых версиях проверка разрешенных java-классов обходится в одном из путей, из-за чего удаленный атакующий может передать специально сформированный сериализованный объект и добиться выполнения произвольного кода.

CVE-2026-32247 (8,1/10) — уязвимость cypher-инъекции в python-пакете Graphiti Core. Злоумышленник может подставить вредоносные значения в SearchFilters.node_labels через MCP или через prompt injection в LLM-клиенте, что приводит к внедрению произвольного cypher-кода в запросы к графовой БД.

CVE-2026-3854 (8,7/10) — уязвимость удаленного выполнения кода в GitHub Enterprise Server. Пользователь, имеющий право отправлять изменения в любой репозиторий через git push, может передать специально сформированные push-опции, которые попадают во внутренние служебные заголовки GitHub и позволяют подменять их параметры, что в итоге может привести к выполнению произвольных команд на сервере.

CVE-2025-54328 (10/10) — десятибалльная уязвимость переполнения буфера в стеке при разборе SMS-сообщений формата RP-DATA в модемной части ряда процессоров и модемов Samsung Exynos. Некорректно сформированное SMS может вызвать сбой обработки и приводить к отказу в обслуживании.

CVE-2025-55292 (8,2/10) — уязвимость в прошивке Meshtastic, открытой mesh-сети для обмена сообщениями по радиоканалу. Атакующий в радиусе действия сети может подделать сообщение NodeInfo от имени чужого узла и сообщить другим участникам mesh-сети, что этот узел работает в режиме HAM.

CVE-2026-34940 (8,8/10) — это уязвимость внедрения команд ОС в KubeAI, в которой компонент KubeAI формирует команду для bash -c из URL модели Ollama без безопасной обработки отдельных частей URL.

Топ-5 CVE по количеству эксплойтов и сканеров уязвимостей на GitHub:

Топ-5 CVE по количеству эксплойтов и сканеров уязвимостей		
CVE	**Количество**	**Описание**
CVE-2026-50751	7	Критический обход аутентификации в Check Point Remote Access VPN / Mobile Access при использовании устаревшего IKEv1 — удаленный атакующий может подключиться к VPN без пароля

CVE-2026-31635	6	Уязвимость в подсистеме RxRPC ядра Linux, известная как DirtyDecrypt, где атакующий может отправить специально сформированный сетевой пакет к уязвимому компоненту и вызвать DoS или повысить привилегии до root
CVE-2026-3854	6	Критическая уязвимость удаленного выполнения кода в **GitHub Enterprise Server**
CVE-2026-42167	6	SQL-инъекция в модуле mod_sql FTP-сервера ProFTPD
CVE-2026-4480	6	Критическая уязвимость удаленного выполнения команд в подсистеме печати Samba

Уязвимости, эксплуатируемые по протоколу HTTP2/HTTP3, gRPC и Websocket

Общее количество таких уязвимостей составило 13. Средняя степень критичности по шкале CVSS — 8,1. Каждая из таких уязвимостей имеет свой уникальный CWE и не выделяет фаворита. Наиболее уязвимым продуктом стал NGINX.

Распределение уязвимостей по протоколам эксплуатации:

Значение	Количество	Доля от CVE, %
HTTP/2	5	38,46%
WebSocket	4	30,77%
gRPC	3	23,08%
HTTP/3	1	7,69%

Наиболее интересные, на наш взгляд, уязвимости из этой категории:

CVE-2026-23918 (8,8/10) — уязвимость типа double free в обработке HTTP/2 в Apache HTTP Server, конкретно в модуле mod_http2. Возможные последствия атаки — аварийное завершение рабочих процессов и отказ в обслуживании, также потенциально возможно выполнение кода в контексте пользователя веб-сервера.

CVE-2026-49975 (7,5/10) — уязвимость, известная как HTTP2 Bomb, затрагивающая Apache HTTP Server и приводящая к отказу в обслуживании.

CVE-2026-23918 и CVE-2026-49975 привлекли наибольшее внимание среди исследователей, число опубликованных PoC/сканеров уязвимостей на GitHub — 15 и 11 соответственно.

CVE-2026-42530 (9,2/10) — уязвимость типа use-after-free в модуле HTTP/3 NGINX Open Source. Основное последствие — перезапуск worker-процесса и отказ в обслуживании.

CVE-2026-27778 (8,7/10) — уязвимость высокой степени критичности в WebSocket API системы ePower, используемой для управления зарядной инфраструктурой, которая может привести к отказу сервиса либо осуществить брутфорс-атаку.

CVE-2026-33186 (9,1/10) — критическая уязвимость обхода авторизации в gRPC-Go. Сервер принимает некорректный HTTP/2-путь в псевдозаголовке :path без начального символа /, но все равно направляет запрос к нужному gRPC-методу, что позволяет удаленному атакующему получить доступ к защищенным методам при определенной конфигурации политик.

Сетевые уязвимости, использующие протокол HTTP

Распределение уровней критичности за второй квартал 2026 года среди уязвимостей с использованием HTTP-протокола составили:

Уровни критичности (баллы)	
Максимальный	10
Минимальный	2,0
Средний	8,0

1. Внутренние сетевые уязвимости

Это уязвимости, которые эксплуатируются в пределах доверенной сети или в тех случаях, когда источник запроса находится внутри доверенного периметра инфраструктуры. Для атаки злоумышленник должен уже иметь доступ к

инфраструктуре либо запрос должен инициироваться доверенным пользователем/системой во внешнюю среду.

К данной категории относятся, в частности, сценарии:

- загрузка вредоносных плагинов, расширений и модулей;
- обмен проектами или конфигурациями, содержащими вредоносные данные;
- открытие вредоносной HTML страницы в уязвимом браузере;
- атаки, сфокусированные на взаимодействии между узлами кластера или микросервисами.

Данные уязвимости сложно или невозможно блокировать средствами защиты информации типа WAF.

Рассмотрим пару уязвимостей, которые получили PoC подтверждения, в качестве примеров.

CVE-2026-0908 (8,8/10) — уязвимость нулевого дня в ChromeANGLE типа Use-After-Free позволяла удаленному злоумышленнику потенциально использовать повреждение кучи через специально созданную HTML-страницу.

CVE-2026-8390 (7,3/10) — это уязвимость Use-After-Free (использование после освобождения) в компоненте JavaScript: WebAssembly браузера Mozilla Firefox. Проблема позволяет удаленному злоумышленнику выполнить произвольный код через специально сформированный WebAssembly-контент.

CVE-2026-5817 (8,6) — это уязвимость в Docker Desktop, которая позволяет выполнить код на хост-системе из контейнера. Проблема связана с недостаточной изоляцией компонента Docker Model Runner на macOS, в частности бэкенда вывода vllm-metal.

CVE-2026-8389 (8,8/10) — это критическая уязвимость в браузере Mozilla Firefox, связанная с неправильной компиляцией в JIT-компиляторе (Just-In-Time) движка JavaScript. Она может привести к удаленному выполнению кода (Remote Code Execution) на устройстве пользователя при посещении вредоносного веб-сайта.

CVE-2026-11645 (8,8/10) — это уязвимость нулевого дня в движке JavaScript V8 браузера Google Chrome. При обработке специально созданной HTML-страницы злоумышленник может вызвать повреждение памяти и обойти защиту «песочницы» браузера.

CVE-2026-49492 (8,8/10) — это уязвимость командной инъекции (OS Command Injection) в популярном расширении для Visual Studio Code Markdown Preview Enhanced. На системах Windows злоумышленник может создать специально сформированный markdown-документ. Если вставить вредоносную команду в атрибуты, например в ссылку mailto:a%26%20calc.exe, после декодирования она превращается в mailto:a& calc.exe. Cmd.exe выполнит calc.exe как вторую команду, что приведет к выполнению произвольного кода в момент предпросмотра документа.

CVE-2026-45504 (8,8/10) — проблема возникает из-за недостаточной валидации в

процессе генерации URL-адресов для предпросмотра документов (WAC), когда Exchange интегрируется с SharePoint и WOPI. В уязвимом потоке Exchange использует функции, которые выполняют HTTP-запросы к URL-адресам, потенциально управляемым злоумышленником, и парсят OData XML-ответ. Суть в том, что Exchange не проверяет схему URL-адреса WebApplicationUrl, возвращаемого WOPI-провайдером.

2. Внешние: WEB-уязвимости

Под внешними мы подразумеваем уязвимости из классического OWASP Top-10 (например, Injection, XSS, CSRF, SSRF), эксплуатируемые удаленно через публичный HTTP-/HTTPS-трафик из интернета. Атакующий не требует начального доступа и напрямую взаимодействует с приложением. Эти угрозы эффективно обнаруживаются и блокируются WAF на основе сигнатур, поведенческого анализа.

Интересные уязвимости

CVE-2026-41940 (9,8/10) — это критическая уязвимость обхода аутентификации в панелях управления хостингом cPanel и WHM, позволяющая неаутентифицированному удаленному злоумышленнику получить полный административный доступ к серверу.

CVE-2026-42945 (9,2/10), также известная как NGINX Rift, — это критическая уязвимость типа «переполнение кучи» в модуле ngx_http_rewrite_module веб-сервера NGINX. Она позволяет неаутентифицированному удаленному злоумышленнику вызвать отказ в обслуживании (DoS) или, при определенных условиях, выполнить произвольный код.

CVE-2026-48907 (9,8/10) — это критическая уязвимость неаутентифицированного удаленного выполнения кода (RCE) в расширении Joomla Content Editor (JCE) для CMS Joomla.

CVE-2026-34197 (8,8/10) — это уязвимость удаленного выполнения кода (RCE) в брокере сообщений Apache ActiveMQ Classic.

CVE-2026-22553 (9,2/10) — это критическая уязвимость OS Command Injection (внедрение команд операционной системы) в SCADA-системе InSAT MasterSCADA BUK-TS, которая позволяет неаутентифицированному удаленному злоумышленнику выполнить произвольный код на сервере.

CVE-2026-41729 (8,1/10) — это уязвимость инъекции языка выражений Spring (SpEL) в проекте Spring Data REST.

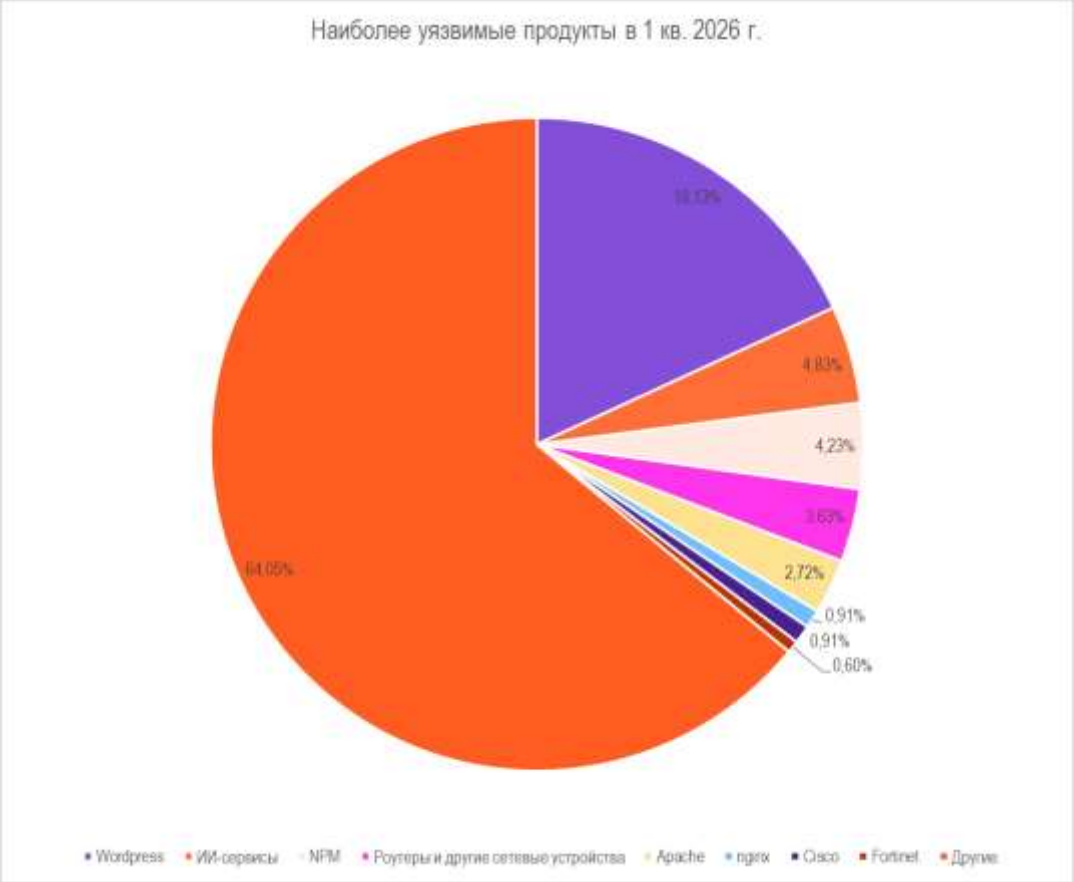
CVE-2026-53435 (8,8/10) — это уязвимость десериализации, которая позволяет авторизованному пользователю читать произвольные файлы в Jenkins.

CVE-2026-10520 (10/10) — уязвимость внедрения команд операционной системы в Ivanti Sentry позволяет удаленному неаутентифицированному пользователю выполнить удаленный код с правами root.

Уязвимости в продуктах, эксплуатируемых по протоколу HTTP

Данный раздел сконцентрирован на уязвимостях, которые могут эксплуатироваться злоумышленником из внешней сети интернет. Ниже продемонстрирована таблица для наиболее критичных сервисов, вендоров и продуктов, в данном квартале мы выделили:

В предыдущем квартале топ выглядел следующим образом:



Как видно на графиках, распределение продуктов осталось примерно таким же. Wordpress и плагины для него остаются продуктом, испытывающим повышенное внимание исследователей безопасности. Хотя в абсолютном выражении (как видно на таблице ниже) количество уязвимостей в Wordpress выросло примерно на 50%, количество уязвимостей в ИИ-сервисах выросло вдвое, как и в библиотеках и фреймворках из NPM.

Продукт	Количество уязвимостей в 2 кв.	Количество уязвимостей в 1 кв.
Wordpress	92	60
ИИ-сервисы	33	16
Библиотеки и фреймворки из Node Package Manager (NPM)	25	14
Роутеры и сетевые устройства	16	12
Продукты компании Apache	12	9
Продукты компании Fortinet	6	2
Продукты компании Cisco	5	3
Joomla	5	-
cPanel	4	-
Продукты компании Nginx	2	3
Другие	314	212

Разберем подробнее уязвимости в этой категории.

Content Management Systems

Данный раздел посвящен уязвимостям в CMS платформах, которые удалось обнаружить во втором квартале 2026 года. На первом месте по количеству обнаруженных PoC занимает CMS Wordpress из-за его обширной библиотеки плагинов и тем. Помимо Wordpress, также были найдены уязвимости в CMS Joomla и CMS Drupal.

Ниже представлено распределение критичности для Wordpress, так как он является наиболее массовым.

Распределение CVSS Wordpress				
Critical	High	Medium	Low	not defined

43	34	15	0	20

Уровни критичности (баллы)	
Максимальный	10
Минимальный	4,3
Средний	8,5

Примеры уязвимостей с максимальным баллом критичности для каждой из CMS:

Wordpress

CVE-2026-8181 (9,8/10) — это критическая уязвимость обхода аутентификации в плагине Burst Statistics для WordPress, позволяющая неаутентифицированному злоумышленнику получить полный административный доступ к сайту.

CVE-2025-29009 (10/10) — это уязвимость типа «неограниченная загрузка файлов опасного типа» в плагине Medical Prescription Attachment Plugin for WooCommerce от Webkul

CVE-2026-49777 (10/10) — это критическая уязвимость в коммерческом wordpress-плагине Product Slider Pro for WooCommerce, позволяющая неаутентифицированному удаленному злоумышленнику выполнить произвольный код на сервере.

CVE-2026-49060 (9,8/10) — это критическая уязвимость типа «некорректное назначение привилегий» в плагине Hippoo Mobile App for WooCommerce для Wordpress, позволяющая неаутентифицированному злоумышленнику выполнить повышение привилегий вплоть до получения прав администратора.

CVE-2026-7567 (9,8/10) — это критическая уязвимость обхода аутентификации в wordpress-плагине Temporary Login (от разработчика elemntor), позволяющая неаутентифицированному злоумышленнику получить доступ к аккаунту любого активного временного пользователя.

CVE-2026-27542 (9,8/10) — это критическая уязвимость типа «некорректное назначение привилегий» (CWE-266) в wordpress-плагине WooCommerce Wholesale Lead Capture, которая позволяет неаутентифицированному злоумышленнику получить права администратора на сайте.

Joomla

CVE-2026-48908 (10/10) — это критическая уязвимость неаутентифицированной загрузки и удаленного выполнения кода (RCE) в популярном конструкторе страниц SP Page Builder для Joomla.

CVE-2026-49048 (9,8/10) — это критическая уязвимость типа «SQL-инъекция» в joomla-компоненте JoomCCK, позволяющая неаутентифицированному удаленному злоумышленнику выполнять произвольные SQL-запросы к базе данных сайта.

CVE-2026-48909 (9,5/10) — это критическая уязвимость, связанная с небезопасной десериализацией PHP в компоненте SP LMS (com_splms) для Joomla.

Drupal
CVE-2026-9082 (6,5/10) — это критическая уязвимость SQL-инъекции (CWE-89) в ядре Drupal.

ИИ-сервисы и агенты

Распределение критичности

Распределение CVSS AI				
Critical	High	Medium	Low	not defined
11	0	9	1	0

Уровни критичности (баллы)	
Максимальный	10
Минимальный	3,7
Средний	8,0

CVE-2026-5027 (8,8/10) — это критическая уязвимость типа Path Traversal (обход пути) в платформе для разработки AI-приложений Langflow, позволяющая неаутентифицированному злоумышленнику выполнить произвольный код на сервере.

CVE-2026-22738 (9,8/10) — это критическая уязвимость в Spring AI, которая позволяет неаутентифицированному злоумышленнику удаленно выполнить код через инъекцию языка выражений Spring (SpEL). Все из-за того, что компонент SimpleVectorStore без должной обработки подставляет данные пользователя в выражение SpEL.

CVE-2026-34156 (9,9/10) — это критическая уязвимость типа «побег из песочницы» (Sandbox Escape) в платформе NocoBase, позволяющая аутентифицированному злоумышленнику выполнить произвольный код на сервере с правами root.

CVE-2026-28363 (9,9/10) — это критическая уязвимость обхода проверки безопасности в OpenClaw, позволяющая аутентифицированному пользователю выполнять команды без требуемого одобрения.

CVE-2026-35570 (8,8/10) — это уязвимость обхода песочницы (пути) в инструменте командной строки OpenClaude, позволяющая локальному пользователю с низкими

привилегиями читать и записывать файлы за пределами ограниченной директории, полностью обходя файловую изоляцию.

CVE-2026-41303 (8,8/10) — это уязвимость обхода авторизации в OpenClaw, которая позволяет пользователям Discord, не входящим в список утверждающих, одобрять ожидающие выполнения команды на хосте.

CVE-2026-42231 (8,8/10) — это критическая уязвимость в платформе автоматизации рабочих процессов n8n, связанная с загрязнением прототипа (Prototype Pollution). Она позволяет аутентифицированному злоумышленнику с правами на создание или изменение рабочих процессов выполнить произвольный код на сервере.

CVE-2026-42048 (9,6/10) — это уязвимость типа Path Traversal (обход пути) в API управления базами знаний платформы Langflow, позволяющая аутентифицированному злоумышленнику удалять произвольные директории на сервере.

CVE-2026-53753 (9,8/10) — это критическая уязвимость в Crawl4AI с открытым исходным кодом и предназначенным для использования с LLM веб-краулером и парсером. Она позволяет неаутентифицированному удаленному злоумышленнику выполнить произвольный код на сервере.

CVE-2026-44789 (9,4/10) — это критическая уязвимость типа «загрязнение прототипа» (Prototype Pollution) в платформе автоматизации n8n, которая позволяет аутентифицированному пользователю с правами на создание или редактирование рабочих процессов (workflows) выполнить произвольный код на сервере.

Уязвимости в пакетах NPM (Node Package Manager)

В библиотеках для node.js также были зафиксированы уязвимости, большая часть из них имели высокий уровень опасности.

Распределение CVSS NPM				
Critical	High	Medium	Low	not defined
4	12	6	2	1

Уровни критичности (баллы)	
Максимальный	9,8
Минимальный	2,1
Средний	7,2

О большом количестве найденных уязвимостей в Next.js мы сообщали в нашем TG-канале.
axios — supply-chain-атака описана в соответствующем разделе.
CVE-2026-9277 (9,2) — это уязвимость командной инъекции (Command Injection) в популярной Node.js-библиотеке shell-quote, которая используется для парсинга и безопасного экранирования команд оболочки.

CVE-2026-30951 (7,5/10) — это уязвимость типа «SQL-инъекция» в популярной ORM-библиотеке для Node.js Sequelize. Уязвимость возникает при обработке JSON-/JSONB-данных в выражениях where.

Уязвимости в роутерах и другом сетевом оборудовании

В данном разделе приведем ряд уязвимостей, которые были обнаружены в различном сетевом оборудовании, маршрутизаторах, ip камерах и т. д.
Распределение критичности следующее:

Распределение CVSS Net. devices				
Critical	High	Medium	Low	not defined
2	11	2	0	1

Уровни критичности (баллы)	
Максимальный	10
Минимальный	6,2
Средний	7,9

CVE-2026-34473 (7,5/10) — это уязвимость типа «отказ в обслуживании» (DoS) в веб-интерфейсах более чем 17 моделей роутеров ZTE ZXHN. Она позволяет неаутентифицированному удаленному злоумышленнику одним запросом сделать интерфейс управления недоступным до перезагрузки устройства.

CVE-2026-34474 — это критическая уязвимость типа «раскрытие конфиденциальной информации» в роутерах ZTE ZXHN моделей H298A 1.1 и H108N 2.6. Она позволяет неаутентифицированному удаленному злоумышленнику получить административный пароль и пароль вайфая (WLAN PSK) одним GET-запросом.

CVE-2026-11499 (9,8/10) — это критическая уязвимость типа стекового переполнения буфера (Stack-based Buffer Overflow) в маршрутизаторах Tenda моделей HG7, HG9 и HG10 с прошивкой 300001138_en_xpon. Она позволяет неаутентифицированному удаленному злоумышленнику выполнить произвольный код на устройстве.

CVE-2026-22226 — это уязвимость типа командной инъекции (OS Command Injection) в модуле конфигурации VPN-сервера роутеров TP-Link Archer BE230 и Archer AX73.

Уязвимости в Apache и Nginx

Большая часть всех найденных уязвимостей имеет критически высокий уровень опасности.
Распределение критичности следующее:

Распределение CVSS Nginx и Apache				
Critical	High	Medium	Low	not defined
5	6	3	0	0

Уровни критичности (баллы)	
Максимальный	10
Минимальный	5,3
Средний	7,9

Кратко опишем часть самых критичных.
CVE-2026-31908 (9,1/10) — это критическая уязвимость типа Header Injection (внедрение HTTP-заголовков) в плагине forward-auth-шлюза API Apache APISIX.

CVE-2026-41873 (9,8/10) — это критическая уязвимость типа HTTP Request Smuggling (CWE-444) в lua-реализации почтового архиватора Apache Pony Mail. Проблема позволяет неаутентифицированному удаленному злоумышленнику захватить учетную запись администратора.

CVE-2026-43512 (9,8/10) — это критическая уязвимость обхода аутентификации (Authentication Bypass) в веб-сервере Apache Tomcat, связанная с механизмом DIGEST-аутентификации.

CVE-2026-33032 (9,8/10) — это критическая уязвимость обхода аутентификации (CWE-306) в веб-интерфейсе управления Nginx nginx-ui, позволяющая неаутентифицированному удаленному злоумышленнику полностью захватить управление над nginx-сервером.

CVE-2026-27654 (8,8/10) — это уязвимость типа Heap-based Buffer Overflow (переполнение динамической памяти) в модуле ngx_http_dav_module веб-сервера NGINX (Open Source и Plus). Она позволяет неаутентифицированному удаленному злоумышленнику вызвать отказ в обслуживании (DoS) и, при определенных условиях, модифицировать имена файлов вне корневого каталога сайта.

Уязвимости в Cisco, Fortinet,citrix и т. д.

Во втором квартале стало известно о нескольких уязвимостях в продуктах от известных в мире информационной безопасности вендоров.

Распределение критичности следующее:

Распределение CVSS Cisco и Fortinet etc.				
Critical	High	Medium	Low	not defined
8	5	2	0	0

Уровни критичности (баллы)	
Максимальный	10
Минимальный	6,5
Средний	8,9

CVE-2026-20223 (10/10) — это критическая уязвимость обхода аутентификации (CWE-306) в продукте Cisco Secure Workload (ранее Cisco Tetration), которая позволяет неаутентифицированному удаленному злоумышленнику получить права администратора сайта (Site Admin) через внутренние REST API.

CVE-2026-0257 (9,1/10) — критическая уязвимость обхода аутентификации в VPN-решении GlobalProtect для Palo Alto Networks PAN-OS и Prisma Access. Она позволяет неаутентифицированному удаленному злоумышленнику подделать сессионные cookie и установить несанкционированное VPN-соединение для доступа к внутренней сети.

CVE-2026-20230 (8,6/10) — это критическая уязвимость типа Server-Side Request Forgery (SSRF) в продуктах Cisco Unified Communications Manager (Unified CM) и Unified CM Session Management Edition (SME). Уязвимость позволяет неаутентифицированному удаленному злоумышленнику записывать файлы в операционную систему устройства, что впоследствии может привести к повышению привилегий до уровня root.

CVE-2026-25089 (9,8) — это критическая уязвимость типа командной инъекции (OS Command Injection) в веб-интерфейсе продуктов FortiSandbox, FortiSandbox Cloud и FortiSandbox PaaS. Она позволяет неаутентифицированному удаленному злоумышленнику выполнить произвольные команды на устройстве через специально сформированные HTTP-запросы.

CVE-2025-66391 (8,8/10) — это уязвимость некорректного контроля доступа в облачной платформе Citrix Cloud, которая позволяет пользователям с правами только на чтение инициировать рабочие процессы для операций записи, например сброс пароля.

cPanel

В популярной графической панели управления веб-хостингом было обнаружено несколько критичных уязвимостей.

CVE-2026-41940 (9,8/10) — критическая уязвимость обхода аутентификации в cPanel & WHM. Позволяет неаутентифицированному удаленному злоумышленнику получить полный административный доступ к серверу.

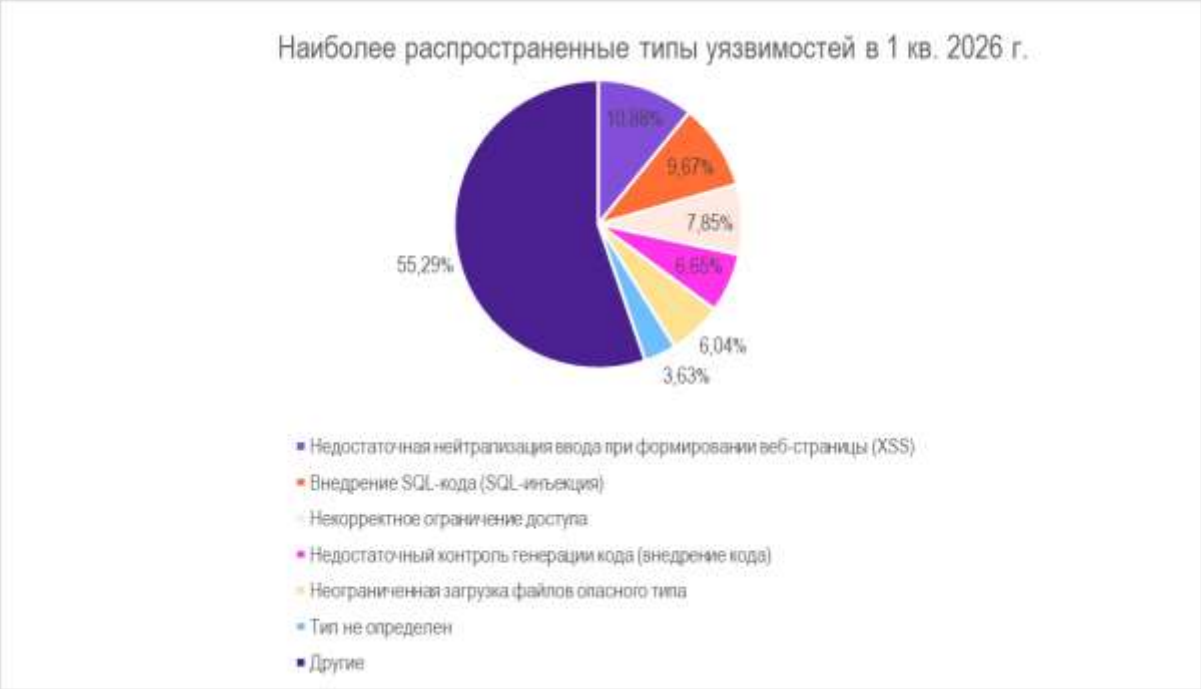
CVE-2026-41940 (10/10) — уязвимость в LiteSpeed User-End cPanel Plugin, позволяющая пользователю cPanel выполнить произвольные скрипты с root-правами.

CVE-2026-48172 (9,8) — это критическая уязвимость повышения привилегий в плагине LiteSpeed User-End cPanel Plugin.

Статистика CWE

Данная таблица полностью совпадает с таблицей прошлого квартала, за исключением количества уязвимостей. CWE-434 часто попадает в топ из-за большого количества уязвимых плагинов Wordpress. XSS и SQLi просто являются самыми базовыми уязвимостями, которые часто находят.

В первом квартале картина наиболее распространенных типов уязвимостей была примерно такой же:



Далее опишем наиболее характерные уязвимости для каждого типа.

CWE HTTP (в штуках)		
CWE	Описание	Кол.во
79	Недостаточная нейтрализация ввода при формировании веб-страницы (XSS)	36
89	Внедрение SQL-кода (SQL-инъекция)	33
22	Уязвимость обхода путей	26
94	Недостаточный контроль генерации кода (внедрение кода)	14
434	Неограниченная загрузка файлов опасного типа	13

CWE-79

CVE-2025-66024 (9/10) — название блог-поста не экранируется в HTML-теге <title>. Злоумышленник с правами на создание постов может внедрить JavaScript в XWiki Blog Application.

CVE-2025-67876 (5,4/10) — пользователь с правами Manage Groups может внедрить JavaScript в названия ролей групп в ChurchCRM.

CWE-89

CVE-2025-59213 (8,8/10) — SQL-инъекция в Microsoft Configuration Manager, позволяющая локальному неавторизованному злоумышленнику повысить привилегии.

CVE-2026-8054 (10/10) — неаутентифицированная SQL-инъекция в dotCMS Core через API-эндпоинты /api/auditPublishing/get и /api/auditPublishing/getAll. Позволяет удаленно читать, изменять и уничтожать данные в БД.

BDU:2025-02933 (9,9/10) — SQL-инъекция в средстве управления проектами Kaiten из-за уязвимости реализации службы запросов Hibernate.

CWE-434

CVE-2026-38526 (9,9/10) — уязвимость, связанная с аутентифицированной произвольной загрузкой файлов в конечной точке /admin/tinymce/upload системы Webkul Krayin CRM.

CVE-2026-21628 (9,8/10) — неправильно защищенная функция управления файлами позволяет неавторизованным пользователям загружать опасные типы данных, что приводит к удаленному выполнению кода.

CWE-22

CVE-2026-27886 (7,5/10) — из-за недостаточной очистки параметров запроса в публичном Content API, неаутентифицированный злоумышленник может использовать параметр where для выполнения атаки типа «булевый оракул» над полями таблицы администраторов (admin_users). Путем подбора символов токена сброса пароля (resetPasswordToken) атакующий может извлечь его и захватить аккаунт суперадминистратора.

CVE-2026-24849 (9,9/10) — уязвимость в методе disposeDocument() файла EtherFaxActions.php позволяет любому аутентифицированному пользователю (независимо от его прав) читать произвольные файлы с сервера, используя специально сформированный параметр file_path.

CWE-94

CVE-2026-47668 (10/10) - Неаутентифицированное выполнение кода в JSON-скрипт-раннере. Атакующий вставляет вредоносный код в параметр functionName, который подставляется в генерируемый JavaScript-код и выполняется в дочернем процессе Node.js в DbGate.

CVE-2026-45829 (10/10) — неаутентифицированное выполнение кода в API-сервере Python. При создании коллекции сервер загружает и выполняет модель с Hugging Face, указанную в запросе, до того, как проверит аутентификацию в ChromaDB.

CVE-2026-44262 (9,4/10) — выполнение PHP-кода в генераторе API-документации для Laravel. Во время генерации документации обрабатываются пользовательские данные из правил валидации, что приводит к выполнению PHP-кода.

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

CVE	описание	Value
CVE-2026-41940	Критическая уязвимость обхода аутентификации в панелях управления хостингом cPanel	71
CVE-2026-42945	Критическая уязвимость типа «переполнение кучи» в модуле ngx_http_rewrite_module веб-сервера NGINX	42
CVE-2026-48907	Критическая уязвимость неаутентифицированного удаленного выполнения кода (RCE) в расширении Joomla Content Editor (JCE) для CMS Joomla	15
CVE-2026-34197	Уязвимость удаленного выполнения кода (RCE) в брокере сообщений Apache ActiveMQ Classic	13
CVE-2026-8181	Критическая уязвимость обхода аутентификации в плагине Burst Statistics для WordPress	11

Вместо заключения: Axios Supply Chain Attack

Как видно из нашего обзора, ситуация на ландшафте эксплойтов в популярном софте от квартала к кварталу меняется мало. Стартовавший в конце года тренд на рост числа уязвимостей в ИИ-сервисах продолжается, их стало почти вдвое больше, чем кварталом ранее. Wordpress, в связи с популярностью и развитостью экосистемы, остается наиболее «многочисленным» по числу эксплойтов ПО. Мы рекомендуем следить за своей ИТ-инфраструктурой и вовремя устанавливать обновления.

Впрочем, во втором квартале стало ясно, что «вовремя» совсем не обязательно означает, что обновления нужно ставить максимально быстро. Часто главной рекомендацией по защите является оперативное обновление. Действительно, своевременное обновление является ключевым аспектом защиты в 99% случаев. Но бывает тот самый один процент, который вечно все портит.

В этой части хотелось бы кратко рассказать про supply-chain-атаку, которая произошла с библиотекой Axios минувшей весной. Axios — это популярная библиотека (HTTP-клиент), которая используется в JavaScript для отправки сетевых запросов к серверам и получения данных (API-запросы, загрузка файлов и т. д.)
Примерно на рубеже первого и второго квартала стали появляться репозитории и статьи, говорящие об Axios Supply Chain Attack.

Атака условно делилась на шесть стадий.

Первая стадия: злоумышленники получили доступ к учетной записи npm Джейсона Сааймана, ведущего разработчика Axios, обладающей наивысшими правами доступа как к пакету npm, так и к репозиторию GitHub.

Вторая стадия: атакующие (группировка UNC1069) создали поддельный аккаунт nrwise и опубликовали чистую версию пакета-ловушки plain-crypto-js@4.2.0. Это было сделано для того, чтобы у будущего вредоносного пакета была «история» и он не вызывал подозрений у систем безопасности как совершенно новый.

Третья стадия: используя украденный токен, атакующие опубликовали две скомпрометированные версии Axios: 1.14.1 и 0.30.4 (с разницей в 39 минут). В этих версиях не менялся код самого Axios. Вместо этого в файл package.json была добавлена фантомная зависимость — plain-crypto-js@4.2.

Четвертая стадия: при установке скомпрометированного Axios npm автоматически разрешал зависимости и устанавливал plain-crypto-js. Далее срабатывал легитимный механизм npm — postinstall-скрипт, который запускал файл setup.js без какого-либо взаимодействия с пользователем.

Пятая стадия: setup.js определял операционную систему жертвы и отправлял HTTP-POST-запрос на C2-сервер (sfrclak.com:8000) для получения специфичной для платформы полезной нагрузки.

Шестая стадия: после успешной загрузки RAT скрипт проводил

«антикриминалистическую» чистку: удалял setup.js, удалял подмененный package.json и переименовывал чистый файл-заглушку (package.md) обратно в package.json.

Таким образом, быстрое обновление и автоматическая установка новых версий (совет, который часто можно встретить в ИБ-сфере, когда речь заходит о защите от атак через уязвимости) стали основным драйвером массового заражения. Однако из этого не следует, что обновляться не нужно, — старые версии ПО накапливают известные CVE и представляют собой предсказуемую угрозу.

Ключевой вывод: **автоматические обновления допустимы только для критических компонентов (браузеры, антивирусы), но не для библиотек и зависимостей в production-среде**. Для них следует применять отложенное обновление с ручным контролем: изучать changelog, проверять появление новых зависимостей и тестировать в staging-окружении перед выкаткой в прод.

О важных новых уязвимостях мы пишем в нашем телеграм-канале «Четыре луча». За завершившийся квартал мы опубликовали семь разборов, созданных, чтобы помочь коллегам по индустрии быстрее и надежнее защитить свою инфраструктуру.

CVE-2026–34156
Лабораторный эксперимент (CVE-2026–21636)
CVE-2026-33453
CVE-2026–41940
Пак уязвимостей Next.js
CVE-2026-10520
CVE-2026-53435