4RAYS by SOLAR

ОБЗОР УЯЗВИМОСТЕЙ ВЕБ-ПРИЛОЖЕНИЙ

I квартал 2026 г.

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

Ключевые выводы

- Количество обнаруженных уязвимостей в первом квартале 2026 года по сравнению с четвертым кварталом 2025 года выросло на 7% — с 397 до 426. В основном рост обусловлен тем фактом, что многие уязвимости, сообщения о которых в публичном доступе появились в 2026 году, были обнаружены еще в 2025 году.
- Сетевой вектор имели 83,84% обнаруженных уязвимостей. В четвертом квартале 2025 года этот показатель составлял 81%.
- Средний уровень критичности обнаруженных сетевых уязвимостей составил 8,1 балла. В четвертом квартале — 7,8, а годом ранее, по итогам первого квартала 2025 года, — 7,3.
- 91,62% всех обнаруженных сетевых уязвимостей эксплуатируются через HTTP. Ближайший «преследователь» — TCP (3,07%).
- На уязвимости уровня Critical и High в совокупности пришлось 72,06% — это заметно выше показателя четвертого квартала 2025 года (69,3%), но лишь не намного выше, чем было в первом квартале (71,5%).
- Самым уязвимым продуктом уже несколько кварталов подряд остается WordPress и плагины для него (18,13%). Доля таких уязвимостей в общем объеме выросла на 4,7 процентных пункта в сравнении с четвертым кварталом. Однако в сравнении с первым кварталом, когда на WordPress приходилось 22,4% уязвимостей, она упала.
- После спада в четвертом квартале вновь вернулась к росту доля уязвимостей в ИИ-сервисах. На них пришлось 4,83%. Примечательно, что в среднем уровень критичности уязвимостей в таких продуктах — 9,2 балла. Это самый высокий показатель среди продуктов-лидеров по количеству обнаруживаемых уязвимостей. Их находят сравнительно редко, но большинство из таких брешей имеют высокий уровень критичности.

Краткая справка

В первом квартале мы проанализировали 426 сообщений о новых уязвимостях и proof-of-concept (PoC) для них в более чем 250 продуктах. Количество сетевых уязвимостей составило 358. Анализировались не только уязвимости 2026 года, но и 2025-го, которые были опубликованы в новом году. Количество PoC уязвимостей из 2025 года составило 173.

В этом отчете мы поделимся результатами нашего анализа сетевых уязвимостей. Особо отметим, что все описанные ниже уязвимости имеют подтверждение, а значит, могут представлять реальную опасность.

В первой части отчета опишем уязвимости, не связанные с протоколом HTTP, о котором отдельно поговорим во второй части отчета, так как он является доминирующим протоколом доставки полезной нагрузки.

Общая статистика по всем сетевым уязвимостям

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

Протокол	**Count**	**%**
HTTP	331	91,62
TCP	11	3,07
Telnet	3	0,84
DNS	2	0,56
Bluetooth Low Energy	2	0,56
Другие	12	3,35

В категорию «Другие» вошли единичные случаи, включающие прикладные протоколы Mongo, gRPC, SSH, DCE/RPC, SMTP, FTP, SMB, DVRIP, транспортный протокол UDP, а также технологии беспроводной связи Wi-Fi, LTE, Bluetooth, используемые в отдельных сценариях эксплуатации.

Распределение критичности уязвимостей, включая сетевой вектор.

Распределение сетевых уязвимостей по степени критичности (количество)				
Critical	High	Medium	Low	not defined
127	131	78	2	20

Уровни критичности (баллы)	
Максимальный	10
Минимальный	2,3
Средний	8,1

Количество десятибалльных уязвимостей, имеющих сетевой вектор: 17

В нашем формальном разделении сетевые уязвимости подвержены рискам, связанным с различными протоколами L1/L7-уровней модели OSI, но не с протоколом HTTP. Общее число таких уязвимостей за квартал — 30, средняя степень их критичности составила 8.1 по шкале CVSS. Самой распространенной CWE стала CWE: 78 (внедрение команд ОС). Наиболее уязвимым продуктом в этой категории был telnetd из пакета GNU Inetutils, который выделяется двумя критическими уязвимостями:

- CVE-2026-24061 (9,8/10) — представляет собой критическую проблему в демоне telnetd, которая возникает из-за недостаточной проверки переменной окружения USER и позволяет удаленно обойти аутентификацию и получить root-доступ. Уязвимость имела широкую популярность среди исследователей, набрав большое число proof of concept и сканеров уязвимости на Github. Более подробно об этой уязвимости мы писали в нашем канале «Четыре луча».

- CVE-2026-32746 (9,8/10) — уязвимость, приводящая к переполнению буфера, а в некоторых случаях и выполнению произвольного кода с правами root без аутентификации, которая находится в обработчике опции LINEMODE. Более подробно читайте в нашем канале.

Перейдем к другим интересным уязвимостям из этой категории, которые привлекли наше внимание:

- CVE-2026-25130 (9,6/10) — это command injection в функциях Cybersecurity AI. Cybersecurity AI — это open-source-фреймворк, который предназначен для автоматизации задач по защите ИИ-систем. Во фреймворке есть набор встроенных инструментов для работы с файлами, командами и другими операциями в хост-системе. Проблема в том, что пользовательский ввод попадает в shell-команды через subprocess.Popen(..., shell=True), что позволяет выполнить произвольные команды на сервере.

- CVE-2026-25770 (9,1/10) — представляет собой критическую эскалацию привилегий в протоколе синхронизации кластера Wazuh Manager, позволяющую аутентифицированным узлам записывать произвольные файлы с правами пользователя wazuh. Из-за небезопасных разрешений по умолчанию этот пользователь может перезаписать основной конфигурационный файл /var/ossec/etc/ossec.conf, внедрив вредоносный блок <localfile>, который выполняется сервисом wazuh-logcollector от root, приводя к удаленному выполнению кода с правами root.

- CVE-2025-14857 (8,8/10), известная как MongoBleed, — критическая уязвимость в MongoDB Server, связанная с неправильной обработкой zlib-сжатых сетевых сообщений. Удаленный неаутентифицированный атакующий может прочитать фрагменты неинициализированной памяти сервера и тем самым получить чувствительные данные.

- CVE-2025-64155 (9,8/10) — критическая уязвимость в Fortinet FortiSIEM, связанная с OS Command Injection. Атакующий может отправить специально сформированный TCP-запрос и получить права root на выполнение команд.

- CVE-2025-14175 (6,0/10) — уязвимость в SSH-сервере роутера TP-Link TL-WR820N версии прошивки v2.80, которая раскрывает содержимое SSH-сессий — команды, пароли, ключи аутентификации и другие передаваемые данные.

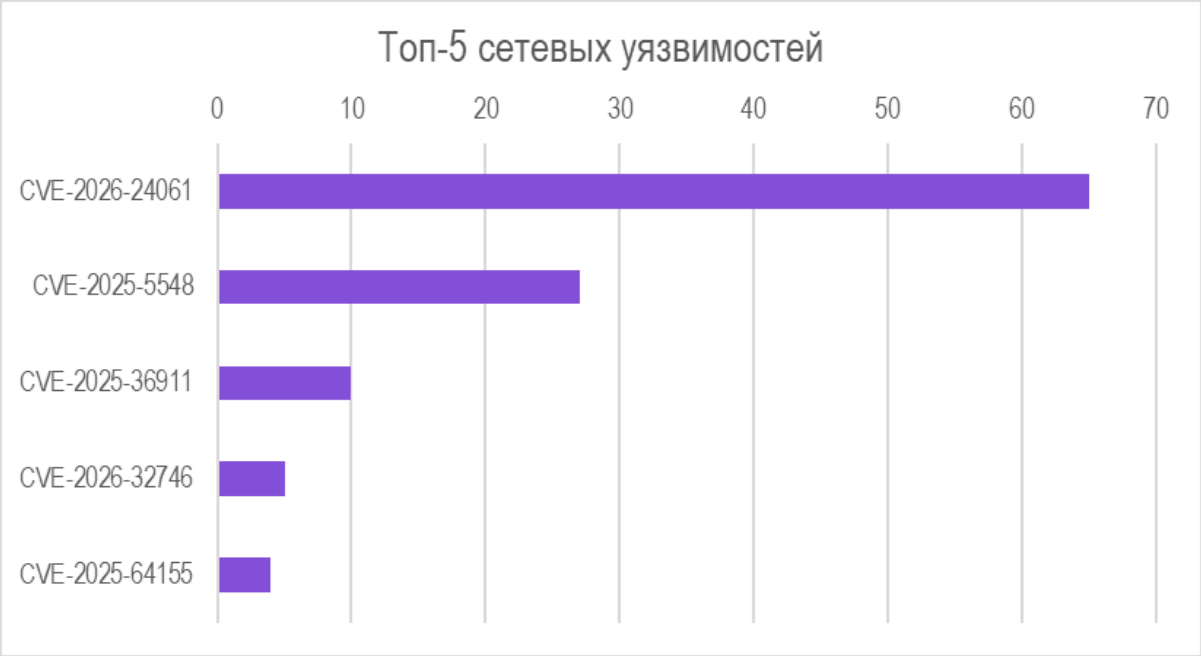
- CVE-2025-36911 (7,1/10) — уязвимость в технологии Google Fast Pair, известная как WhisperPair, которая затрагивает Bluetooth-наушники, гарнитуры и колонки

множества брендов. По опубликованным данным, она может затронуть сотни миллионов устройств по всему миру и позволяет атакующему без физического доступа и без участия пользователя перехватывать сопряжение, получать контроль над аксессуаром и потенциально прослушивать разговоры или отслеживать местоположение.

- CVE-2025-29969 (7,5/10) — уязвимость в Microsoft Windows, связанная с протоколом MS-EVEN RPC. По сути, это ошибка типа TOCTOU, из-за которой авторизованный атакующий может выполнить произвольный код по сети. Уязвимость затрагивает сразу много версий Windows: от старых веток вроде Windows Server 2008/2012 до более новых Windows 10, Windows 11 и Windows Server 2025.

- CVE-2025-68926 (9,8/10) — критическая уязвимость в RustFS, распределенной системе хранения объектов на Rust, позволяющая обойти аутентификацию gRPC с помощью жестко закодированного токена. О ней мы писали подробно.

В данной категории можно выделить топ-5 уязвимостей по числу Proof of Concept и сканеров уязвимостей на Github:



Топ-5 CVE по количеству эксплойтов и сканеров уязвимостей		
CVE	**Количество**	**Описание**
CVE-2026-24061	65	Критическая проблема в демоне telnetd, позволяющая удаленно

		обойти аутентификацию и получить root-доступ
CVE-2025-5548	27	CVE-2025-5548 — это уязвимость средней критичности в FreeFloat FTP Server, связанная с переполнением буфера (CWE-119) в обработчике команды NOOP
CVE-2025-36911	10	Уязвимость в технологии Google Fast Pair
CVE-2026-32746	5	Уязвимость в telnetd, приводящая к переполнению буфера, а в некоторых случаях и к выполнению произвольного кода с правами root
CVE-2025-64155	4	Критическая уязвимость в Fortinet FortiSIEM, связанная с OS Command Injection

Сетевые уязвимости, использующие протокол HTTP

Распределение уровней критичности уязвимостей с использованием HTTP протокола за первый квартал 2026 года:

Максимальный балл критичности	10
Средний уровень критичности	8,1
Минимальный балл критичности	2,3

1. Внутренние 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-2026-25769 (9,1/10) — уязвимость в wazuh, позволяющая злоумышленнику, получившему доступ к рабочему узлу (любыми способами), выполнить полный RCE на главном узле с привилегиями root. Уязвимость возникает из-за того, что функция as_wazuh_object() небезопасно обрабатывает объекты с ключом __callable__:
  - Читает __module__ из пользовательского ввода.
  - Вызывает import_module() без whitelist.
  - Получает любую функцию через getattr().
  - Возвращает и выполняет ее.

  CVE-2026-21852 (5,3/10) — уязвимость в Claude Code, позволяющая похищать данные пользователя, включая ключи API Anthropic, до того, как пользователи подтвердят доверие. Уязвимость возникает вследствие клонирования пользователем вредоносного репозитория и его инициализации через Claude. При init Claude читает конфиг до показа trust-предупреждения и шлет API-запросы (с ключом в header) на сервер контролируемым злоумышленником.

- CVE-2025-59536 (8,5/10) — уязвимость в Claude Code, позволяющая выполнять произвольный код. Уязвимость заключается в том, что при клонировании проекта и открытии его в Claude код выполняется раньше появления диалогового окна с подтверждением доверия к проекту.

- CVE-2026-2441 (8,8) — уязвимость в Google Chrome, позволяющая выполнить удаленный код в песочнице браузера. Суть уязвимости заключается в том, что браузер обращается к уже освобожденному участку памяти. В нормальной работе приложения такие объекты должны корректно удаляться и не использоваться повторно, однако из-за ошибки в логике управления памятью возникает ситуация, при которой ссылка на уже освобожденный объект остается активной.

- CVE-2026-4342 (8,8/10) — уязвимость в ingress-nginx, позволяющая через комбинацию аннотаций Ingress внедрить произвольную конфигурацию в nginx и получить удаленное выполнение кода в контексте контроллера ingress-nginx.

2. Внешние 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 веб-уязвимости

- CVE-2026-21858 (10/10) — уязвимость в путанице типов, позволяющая читать или выполнять произвольные файлы в n8n. Путаница типов возникает, когда злоумышленник подменяет MIME type на application/json или что-то другое. Из-за ошибки Content-Type Confusion вызывается обычный парсер тела (parseBody()), который присваивает данные напрямую в req.body без проверки и защиты.

- CVE-2026-21962 (10/10) — уязвимость удаленного выполнения кода (RCE) в Oracle Fusion Middleware, которые используют Oracle HTTP Server и плагин WebLogic Server Proxy для переадресации веб-трафика на серверы бэкенд-приложений.

- CVE-2026-21721 (8,1/10) — уязвимость небезопасного управления привилегиями в дашбордах Grafana. API отвечает за изменение разрешений дашбордов Grafana и не проверяет корректный контекст целевой панели — он лишь смотрит, есть ли у пользователя базовое право на управление разрешениями. В результате если у пользователя есть право управлять разрешениями хотя бы на одном дашборде, то он может изменить разрешения других дашбордов.

- CVE-2026-27944 (9,8/10) — уязвимость в Nginx UI, позволяющая получить полную резервную копию системы неаутентифицированному злоумышленнику. Она возникает из-за отсутствия механизма проверки аутентификации при обращении к данной конечной точке /api/backup.

- CVE-2026-24858 (9,8/10) — уязвимость, позволяющая обойти аутентификацию в FortiCloud. Злоумышленник, владеющий любой учетной записью FortiCloud, может повторно использовать свой токен SSO для входа в устройства других клиентов.

- CVE-2026-20127 (10/10) — уязвимость нулевого дня в Cisco Catalyst SD-WAN и Cisco Catalyst SD-WAN, позволяющая обойти аутентификацию и получить административные привилегии через запрос к файлу .dca. Подробнее читайте в нашем канале.

- CVE-2026-21876 (9,3/10) — уязвимость в OWASP (CRS) обхода сигнатуры путем перезаписи переменной в TX: значения. Она возникает из-за того, что при переборе нескольких частей в первом правиле цепочки значения TX:0/TX:1

перезаписываются на каждой итерации. Если ранняя часть содержит вредоносный/нетипичный charset, например закодированную полезную нагрузку, а последняя часть — нормальный charset=utf-8, то WAF увидит только последнюю часть.

Уязвимости в продуктах, эксплуатируемых по протоколу HTTP

Ванном разделе представлена информация об уязвимостях, которые могут эксплуатировать злоумышленники из внешней сети (интернета). Ниже дана таблица с наиболее критичными сервисами, вендорами и продуктами, которые мы выделили в 1-м квартале:

Самые уязвимые	
Wordpress	60
ИИ-сервисы	16
Роутеры и другие сетевые устройства	12
Продукты компании Fortinet	2

библиотеки и фреймворки из Node Package Manager (NPM)	14
Продукты компании Apache	9
Продукты компании Nginx	3
Продукты компании Cisco	3

WordPress

Распределение критичности уязвимостей, связанных с Wordpress, его плагинами или темами:

Уровни критичности уязвимостей в WordPress (баллы)	
Максимальный	10
Минимальный	4,3
Средний	7,9

При этом количество критичных уязвимостей является максимальным:

Распределение критичности уязвимостей в Wordpress и плагинах для него (количество)				
Critical	High	Medium	Low	Не определен
24	18	18	0	7

Приведем пример двух уязвимостей, обнаруженных в этом году, с максимальным баллом критичности 10:

- CVE-2025-49071 (10/10) — уязвимость в теме flozen-theme. Уязвима для произвольной загрузки файлов из-за отсутствия проверки типов файлов. CWE-434.

- CVE-2026-23550 (10/10) — уязвимость в плагине Modular DS, позволяющая получить доступ к административной панели. CWE-266

При этом самая распространенная CWE: CWE-434.

ИИ-сервисы и агенты

В данном разделе приведено распределение уязвимостей, связанных с ИИ-ассистентами, чат-ботами и другими сервисами.

Распределение критичности:

Уровень критичности уязвимостей в ИИ-сервисах (баллы)	
Максимальный	10
Минимальный	7,2
Средний	9,2

Как видим, количество критичных уязвимостей в значительной степени больше остальных.

Распределение критичности уязвимостей в ИИ-сервисах (в штуках)				
Critical	High	Medium	Low	Не определен
9	4	0	0	2

Мы описывали выше уязвимости, связанные с ИИ, например CVE-2026-21858 или CVE-2026-25807. Можем отметить и довольно необычную уязвимость, связанную с промпт-инжинирингом, позволявшую обойти политики большинства чат-ботов, например ChatGPT 4.0, DeepSeek v3.2, Gemini 3 Pro. Благодаря атаке, использующей многоуровневые поведенческие переопределения, принудительное переназначение идентификаторов, принуждение выходных данных и преобразование закодированных входных данных для снижения эффективности применения политик. Помимо этой, нами зафиксированы уязвимости в популярных инструментах, связанных с построением ИИ-агентов: langchain, Langflow, n8n и т. д. Об уязвимости Langflow мы недавно рассказывали в нашем телеграм-канале Например.

Самая распространенная CWE: CWE: 94.

Еще немного про ИИ

Общим трендом первого квартала является появление сканеров уязвимостей для популярных ИИ-сервисов. Так, например, по данным одного из них, на март 2026 г. в AI-агенте OpenClaw содержится более 522 CVE, и еженедельные обновления базы продолжаются, что говорит о кризисе безопасности OpenClaw. ClawJacked — это новый вектор атаки на AI-агент.

Уязвимость заключалась в том, что OpenClaw Gateway принимал WebSocket-подключения с localhost без ограничения числа попыток аутентификации и без

обязательного подтверждения нового устройства (pairing). В результате вредоносный сайт, открытый пользователем в браузере, мог установить WebSocket-соединение с локальным gateway и перебрать пароль. После успешной аутентификации OpenClaw автоматически добавлял это подключение как trusted device и выдавал ему постоянный токен доступа. Получив такой доступ, злоумышленник мог выполнять команды, читать конфигурацию и полностью управлять OpenClaw от имени пользователя.

Уязвимости в пакетах NPM (Node Package Manager)

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

Уровни критичности уязвимостей в пакетах NPM (баллы)	
Максимальный	9,8
Минимальный	2,3
Средний	8,2

Распределение критичности:

Распределение критичности уязвимостей в NPM				
Critical	High	Medium	Low	not defined
7	4	2	1	0

- CVE-2025-61686 (9,1/10) — уязвимость в React Router, благодаря которой злоумышленник может заставить сессию попытаться прочитать/записать данные из места за пределами указанного каталога файлов сессии. CWE-22.
- CVE-2026-26830 (9,8/10) — уязвимость в PDF-image, позволяющая выполнить удаленный код через параметр pdfFilePath. CWE-78.
- CVE-2026-26832 (9,8/10) —– уязвимость в node-tesseract-ocr, позволяющая выполнить удаленный код из за передачи данных в child_process.exec() без надлежащей проверки. CWE-78.
- CVE-2026-26833 (9,8/10) — уязвимость в thumbler, из-за которой допускается внедрение команд ОС через параметры input, output, time или size в функции thumbnail(). CWE-94.
- CVE-2026-26831 (9,8/10) — уязвимость в textract, позволяющая выполнить удаленный код из-за небезопасной передачи именами filePath напрямую в child_process.exec(). CWE-78.

Самая распространенная CWE: CWE-78.

Уязвимости в роутерах и другом сетевом оборудовании

В этом разделе мы не учитываем уязвимости в Cisco, Fortinet, Pan-os. Здесь дано описание уязвимостей в различных роутерах, IP-камерах, телефонии и проч.

Уровень критичности уязвимостей в сетевых устройствах (баллы)	
Максимальный	10
Минимальный	5,3
Средний	7,3

Распределение критичности (количество):

Распределение критичности уязвимостей в сетевых устройствах				
Critical	High	Medium	Low	not defined
1	8	2	0	0

Опишем часть наиболее критичных уязвимостей.

- CVE-2025-67160 (7,5/10) — уязвимость, позволяющая злоумышленникам получать доступ к конфиденциальным каталогам и файлам посредством обхода каталогов в IP камерах Vatilon. CWE-22.
- CVE-2026-25857 (8,6/10) — уязвимость, позволяющая выполнять произвольный код в прошивке маршрутизатора Tenda G300-F. CWE-78.
- CVE-2026-0651 (5,3/10) — уязвимость обхода путей в TP-Link Tapo C260 v1 и D235 v1. CWE-22.
- CVE-2025-34037 (10/10) — уязвимость удаленного выполнения кода в маршрутизаторах Linksys серии E. CWE-78.

Самая распространенная CWE: CWE-78.

Уязвимости в Apache и Nginx

Уровень критичности уязвимостей в Apache и Ngnix (баллы)

Максимальный	9,8
Минимальный	6,3
Средний	8,1

Распределение критичности (количество):

Распределение критичности уязвимостей в Nginx и Apache				
Critical	High	Medium	Low	not defined
2	8	2	0	0

- CVE-2025-60021 (9,8/10) — уязвимость удаленного выполнения кода в Apache bRPC во встроенном сервисе профилировщика памяти /pprof/heap. CWE-77.

- CVE-2026-27944 (9,8/10) — писали о ней выше и в нашем телеграм-канале.

Самая распространенная CWE: CWE-20.

Уязвимости в Cisco, Fortinet и Palo Alto

В первом квартале стало известно о нескольких уязвимостях в продуктах от известных в мире информационной безопасности вендоров.

- CVE-2026-20127(10/10) — об этой уязвимости мы уже писали выше и в нашем телеграм-канале. CWE-287.

  CVE-2026-20079 (10/10) — уязвимость в веб-интерфейсе программного обеспечения Cisco Secure Firewall Management Center (FMC), позволяющая неавторизованному удаленному злоумышленнику обойти аутентификацию и выполнить скриптовые файлы на уязвимом устройстве для получения root-доступа к базовой операционной системе.CWE-288.

  CVE-2026-20131 (10/10) — уязвимость в веб-интерфейсе управления программным обеспечением Cisco Secure Firewall Management Center (FMC), позволяющая неавторизованному удаленному злоумышленнику выполнять произвольный код Java с правами root посредством небезопасной десериализации предоставленного пользователем потока байтов Java.CWE-502.

- CVE-2026-24858 (9,8/10) — уязвимость, позволяющая злоумышленнику, владеющему любой учетной записью FortiCloud (бесплатной или платной), повторно использовать свой токен SSO для входа в устройства других клиентов (независимо от версии, указанной ниже), не зная их паролей.CWE-288.

- CVE-2025-4615 (7/10) — уязвимость, связанная с некорректной нейтрализацией входных данных в веб-интерфейсе управления программного обеспечения Palo

Alto Networks PAN-OS, позволяющая авторизованному администратору обходить системные ограничения и выполнять произвольный код. CWE-83.

Статистика CWE

В 1-м квартале 2026 г. удалось выделить топ-5 CWE-уязвимостей, который составлен из общего числа всех проанализированных уязвимостей, эксплуатируемых по протоколу HTTP. Всего из 331 уязвимости 12 не получили CWE-идентификатор по различным причинам, например CVE еще не опубликована в NIST.

CWE HTTP (количество)		
CWE	Описание	Кол.во
79	Недостаточная нейтрализация ввода при формировании веб-страницы (XSS)	36
89	Внедрение SQL-кода (SQL-инъекция)	32
22	Некорректное ограничение доступа	26
94	Недостаточный контроль генерации кода (внедрение кода)	22
434	Неограниченная загрузка файлов опасного типа	20

Процентное соотношение выделенных топ-5 CWE-уязвимостей относительно общей массы всех уязвимостей, имеющих идентификатор, составило: 42,2%.

Кратко изложим примеры CVE, относящихся к топу CWE с максимальным рейтингом критичности.

CWE-79

CVE-2026-30862 (9/10) — уязвимость повышения привилегий за счет хранимой XSS-инъекции в Appsmith.

CWE-89

CVE-2026-26988 (9,3/10) — уязвимость внедрения SQL запросов в LibreNMS.

CWE- 434

Большая часть этих уязвимостей была найдена в плагинах для CMS Wordpress, но есть и другие примеры. CVE-2026-28289 (10/10) — внедрение произвольных файлов в FreeScout.

CWE-22

CVE-2026-30952 (8,7/10) — уязвимость обхода путей в AdonisJS.

CWE-94

CVE-2026-1281 (9,8/10) — внедрение кода в Ivanti Endpoint Manager Mobile.

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

В 1-м квартале 2026 г. рейтинг самых популярных уязвимостей исходя из количества опубликованных эксплойтов выглядит следующим образом.

Топ-5 CVE по количеству эксплойтов		
CVE	**Кол-во**	**Описание**
CVE-2025-2304	17	Уязвимость, приводящая к повышению привилегий путем массового назначения паролей Camaleon CMS
CVE-2026-23744	16	Уязвимость удаленного выполнения кода (RCE), позволяющая злоумышленнику отправлять специально сформированный HTTP-запрос, запускающий установку MCP-сервера и приводящий к RCE в MCPJam Inspector

CVE-2026-21858	11	Уязвимый рабочий процесс может предоставить доступ неаутентифицированному удаленному злоумышленнику, что приведет к раскрытию конфиденциальной информации в n8n
CVE-2026-29000	11	Уязвимость обхода аутентификации в JwtAuthenticator при обработке зашифрованных JWT в pac4j-jwt
CVE-2026-21962	8	Уязвимость удаленного выполнения кода (RCE) в Oracle Fusion Middleware

Заключение

По итогам анализа ландшафта веб-уязвимостей в первом квартале 2026 года мы можем сделать следующие выводы:

1. **HTTP остается главным вектором атак.**
   Фокус защитных мер должен быть направлен на сервисы и приложения, использующие этот протокол. Особое внимание требуется платформам с высокой концентрацией уязвимостей, таким как WordPress.
2. **Векторы атак разнообразны**
   Сетевые уязвимости, не связанные с HTTP-протоколом, демонстрируют разнообразие векторов эксплуатации при относительно небольшом количестве. При этом их средний уровень критичности остается высоким, что обусловлено воздействием на инфраструктурные сетевые сервисы и протоколы.
3. **ИИ-сервисы требуют мониторинга и защиты.**
   Рост числа сканеров и обнаруженных уязвимостей в ИИ-сервисах указывает на возрастающую угрозу. Требуется разработка специализированных механизмов защиты для таких систем.
4. **ИБ-командам следует следить за наиболее распространенными CWE.**
   Топ-5 CWE демонстрируют повторяющиеся слабые места в разработке ПО. Их своевременное устранение снизит риск массовых атак.
5. **Инфраструктуру нужно своевременно обновлять и сегментировать.**
   Высокий уровень критичности обнаруженных уязвимостей подчеркивает необходимость:
   - оперативного выпуска и применения патчей, особенно если речь идет о популярных open-source-решениях;
   - ограничения сетевой доступности сервисов;
   - сегментации инфраструктуры для минимизации последствий атак.
6. **Трафик нужно анализировать, а доступ — контролировать.**
   Для защиты от уязвимостей, не связанных с HTTP, ключевую роль играют средства анализа сетевого трафика и строгий контроль доступа к инфраструктурным сервисам.

7. **Отслеживать появление PoC-эксплойтов — критически важно.**
   Анализ популярности уязвимостей по числу эксплойтов помогает приоритизировать усилия по устранению наиболее опасных сценариев атак.