4RAYS by SOLAR



ОБЗОР СЕТЕВЫХ УЯЗВИМОСТЕЙ

3 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 обнаруженных сетевых уязвимостей в третьем квартале 2026 года.

Ключевые выводы

- Количество обнаруженных уязвимостей в третьем квартале 2026 года по сравнению со вторым кварталом 2026 года выросло на 28,34% — с 681 до 874. **Большой рост количества найденных уязвимостей и опубликованных PoC/exploit на протяжении трех и, скорее всего, последующих кварталов можно связать с полноценным входом AI-инструментов**, которые используются для анализа кода, составления PoC/exploit-скриптов, создания изолированных лабораторных.

- Сетевой вектор имели 87,9% обнаруженных уязвимостей. Во втором квартале таких было 83,84%.

- Средний уровень критичности обнаруженных сетевых уязвимостей составил 8,15 балла. Во втором квартале — 7,9. Медианный же составил 8,7.

- 84,9% всех обнаруженных сетевых уязвимостей эксплуатируются через HTTP. Кварталом ранее таких уязвимостей было 90,2%.

- Сетевые уязвимости уровня Critical и High в совокупности занимают 86,18% от общей массы всех сетевых уязвимостей. Во втором квартале этот показатель составлял 73,5%.

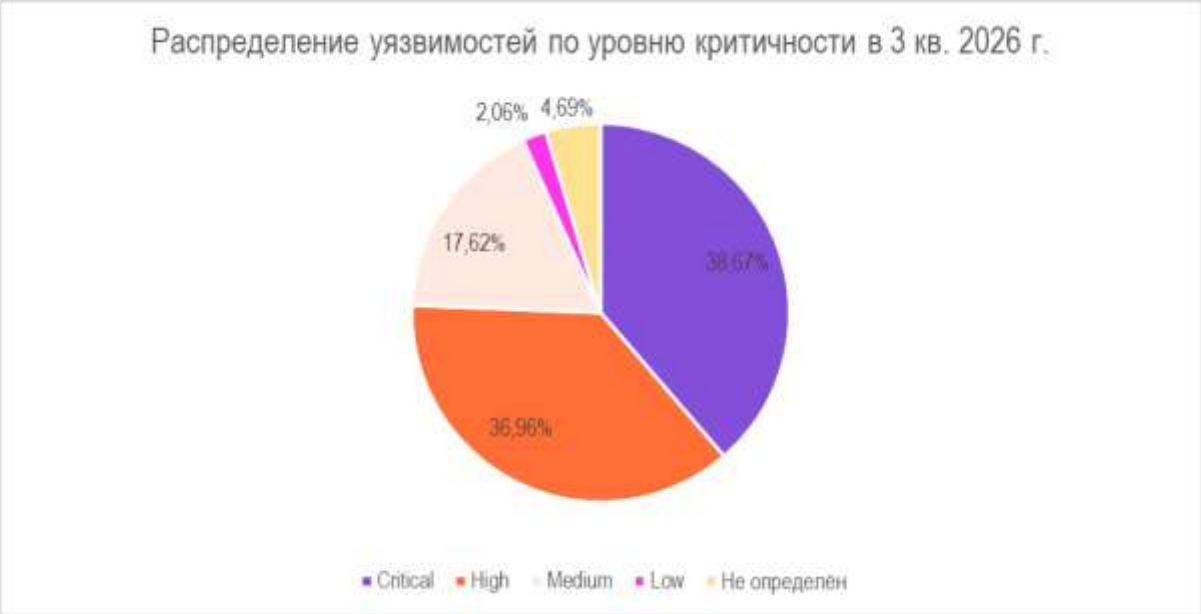
- 45 уязвимостей, имеющих сетевой вектор, получили десятибалльную оценку по шкале CVSS.

- WordPress также топ-1 по количеству опубликованных PoC/exploit-скриптов.

- На AI-сервисы пришлось 7,37% всех сетевых уязвимостей, показатель вырос с 4,83% во втором квартале. Средний уровень критичности — 8,83 (8 — во втором квартале).

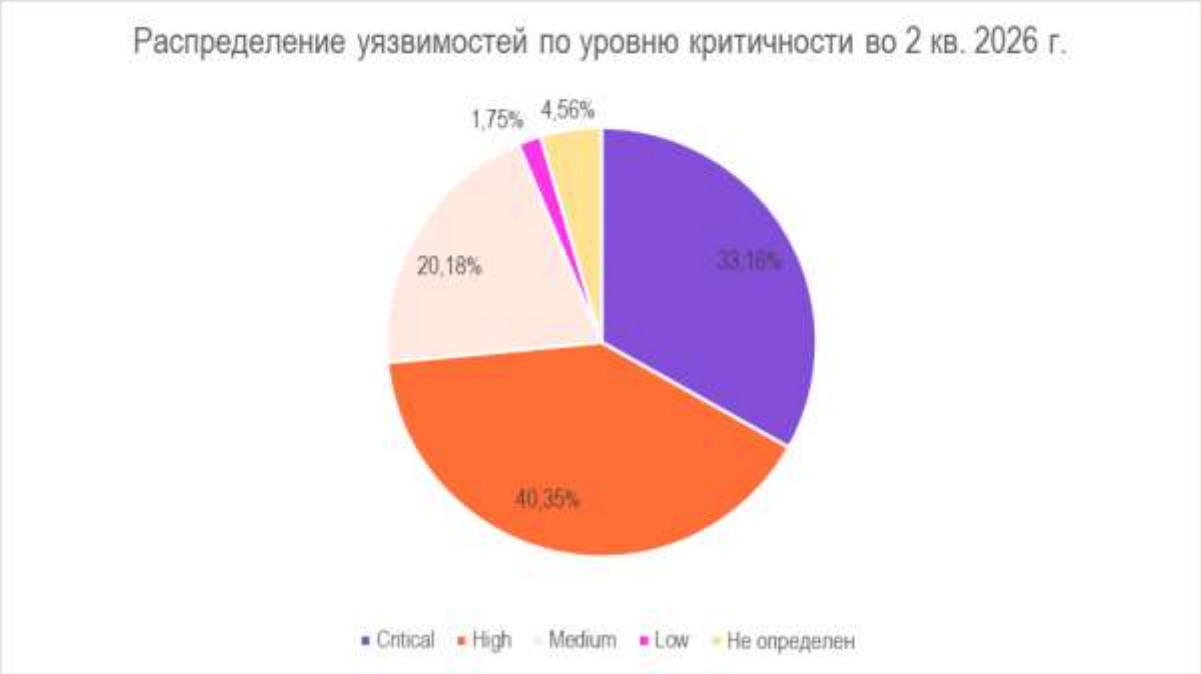
Краткая справка

В третьем квартале наши средства мониторинга обнаружили 874 уязвимости (+295,3% в сравнении год к году) в 569 уникальных продуктах. Из них доля, в которых есть подтвержденный Proof of Concept, — 97,4%. Во всех остальных случаях — сканеры и описания. Средняя критичность составила 8,15, число десятибалльных по шкале CVSS уязвимостей — 44.



Категория	Количество CVE
Critical	338
High	323
Medium	154
Low	18
Без оценки CVSS	41

Во втором квартале критичных уязвимостей было заметно меньше:



В третьем квартале из общего числа уязвимостей сетевой вектор имеют 768 (87,9% от общего числа), из них в 652 протокол эксплуатации — HTTP. О них и расскажем подробнее далее в данном отчете.

Распределение уязвимостей по вектору атаки:



Категория	Количество CVE
network	768

local	94
adjacent	11
physical	1

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

Протокол	CVE	Доля Network
HTTP	652	84,9%
Не определен	54	7%
WEBSOCKET	8	1%
TCP	7	0,9%
HTTP2	4	0,5%
SSH	4	0,5%
POSTGRESQL	3	0,4%
SCTP	3	0,4%
DHCP	2	0,3%
DNS	2	0,3%
SMTP	2	0,3%
UDP	2	0,3%
Другие	**25**	3,2%

Как можно заметить, для значительной части сетевых уязвимостей невозможно однозначно определить протокол передачи данных, поскольку их эксплуатация может осуществляться с использованием различных протоколов и способов доставки полезной нагрузки. Подобная ситуация характерна для уязвимостей библиотек, компонентов обработки входных данных, сетевых стеков и серверных модулей. В этих случаях возможность эксплуатации определяется особенностями приложения, архитектурой системы или конфигурацией уязвимого компонента. Поэтому отнесение

таких уязвимостей к одному конкретному протоколу может привести к некорректной оценке потенциальной поверхности сетевой атаки.

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 104. Средняя критичность — 7,9, медианная — 8,8 по шкале CVSS. Лидирующими CWE стали: CWE: 502 — Deserialization of Untrusted Data, CWE: 77 — Improper Neutralization of Special Elements used in a Command и CWE: 94 — Improper Control of Generation of Code. Наиболее уязвимыми оказались продукты Apache Camel — 18 уязвимостей; OpenSSL, iOS, Linux Kernel — по 4 уязвимости в каждом продукте.

Распределение уязвимостей по присвоенному CWE:



Распределение уязвимостей по присвоенному CWE:

CWE	CVE	Доля от CVE, %
CWE-502	9	8,7
CWE-77	8	7,7
CWE-94	8	7,7
CWE-20	7	6,7
CWE-78	6	5,8
CWE-119	4	3,8
CWE-22	4	3,8
CWE-863	4	3,8
CWE-121	3	2,9
CWE-122	3	2,9
CWE-416	3	2,9
CWE-476	3	2,9
CWE-787	3	2,9
CWE-829	3	2,9

Наиболее интересные, по нашему мнению, уязвимости:

CVE-2026-52993 (9,8/10) — уязвимость типа Double Free (CWE: 415) в подсистеме TIPC Linux kernel. При обработке фрагментированных TIPC-сообщений из-за ошибки управления skb один и тот же буфер может быть освобожден дважды, что приводит к повреждению памяти ядра и потенциальному отказу в обслуживании.

CVE-2026-28576 (10/10) — уязвимость типа SQL Injection (CWE: 89) в Android Contacts Provider. Некорректная обработка SQL-запросов позволяет получить доступ к базе контактов и раскрыть локальные данные без действий пользователя. Уязвима Android 17.

CVE-2026-43682 (9,8/10) — уязвимость выхода за границы буфера (CWE: 119) в ядре macOS, связанная с обработкой структур HFS+. Некорректно сформированные данные HFS+ могут вызвать повреждение памяти ядра и аварийное завершение системы.

CVE-2026-62878 (9,8/10) — уязвимость переполнения буфера в стеке (CWE: 121) в Windows DNS Server. Специально сформированные сетевые данные позволяют неаутентифицированному удаленному атакующему выполнить произвольный код на DNS-сервере.

CVE-2025-14659 (7,4/10) — уязвимость Command Injection (CWE: 77) в DHCP Daemon роутеров D-Link DIR-860LB1 и DIR-868LB1. Изменение параметра Hostname при обработке DHCP lease позволяет удаленному атакующему выполнить произвольные команды на устройстве.

CVE-2026-76578 (9,8/10) — уязвимость отсутствия аутентификации (CWE: 306) в FreeIPA. Неаутентифицированный удаленный клиент через LDAP может создать подконтрольный ему Kerberos principal и добавить его в группу администраторов, получив административные права над FreeIPA/IdM.

CVE-2026-52924 (9,8/10) — уязвимость Use-After-Free (CWE: 416) в SCTP Linux kernel. При обработке некорректного Stale Cookie ERROR ядро освобождает структуру потока, но сохраняет указатель на нее, что может привести к краху ядра (DoS) и потенциально к выполнению произвольного кода.

CVE-2026-42298 (10/10) — критическая уязвимость Code Injection (CWE: 94) в Postiz — AI-платформе для планирования публикаций в социальных сетях. Через специально сформированный Pull Request с измененным Dockerfile.dev злоумышленник может выполнить произвольный код в процессе сборки docker-образа и похитить привилегированный GITHUB_TOKEN.

CVE-2026-27941 (9,9/10) — уязвимость в OpenLIT — open-source-AI-платформе для AI engineering и наблюдаемости LLM-приложений. В GitHub Actions использовался небезопасный pull_request_target, из-за чего код из внешнего fork Pull Request мог выполняться с привилегиями основного репозитория и получать доступ к GITHUB_TOKEN и секретам (CWE: 829 — Inclusion of Functionality from Untrusted Control Sphere).

CVE-2026-38577 (9,8/10) — уязвимость Use of Hard-coded Credentials (CWE: 798) в Tenda HG21 XPON Fiber Modem с прошивкой V4.0.0-260302. В прошивке присутствует статическая учетная запись администратора с root-привилегиями, что позволяет удаленному атакующему получить полный доступ к устройству.

CVE-2026-14662 (8,8/10) — ошибка целочисленного переполнения (CWE: 190) при обработке типов tsvector и tsquery в PostgreSQL. Она приводит к выделению слишком маленького буфера и записи за его пределами, что может привести к RCE.

CVE-2026-14669 (8,8/10) — переполнение heap-буфера (CWE: 122) в функции to_char(timestamptz) PostgreSQL. Специально выбранная длинная POSIX-аббревиатура часового пояса может вызвать повреждение памяти и RCE.

CVE-2026-65400 (9,8/10) — критическая уязвимость обхода аутентификации (CWE: 287) в функции Screen Sharing операционной системы Apple macOS. Удаленный атакующий, имеющий сетевой доступ к службе, может подключиться к Screen Sharing без корректных учетных данных. Уязвимость затрагивает screensharingd и используется через TCP/5900.

CVE-2026-25243 (7,7/10) — уязвимость Heap-based Buffer Overflow (CWE: 122) в Redis. Ошибка в проверке сериализованных данных команды RESTORE позволяет аутентифицированному атакующему с правом выполнения этой команды передать специально сформированный объект, вызвать повреждение памяти и потенциально выполнить произвольный код.

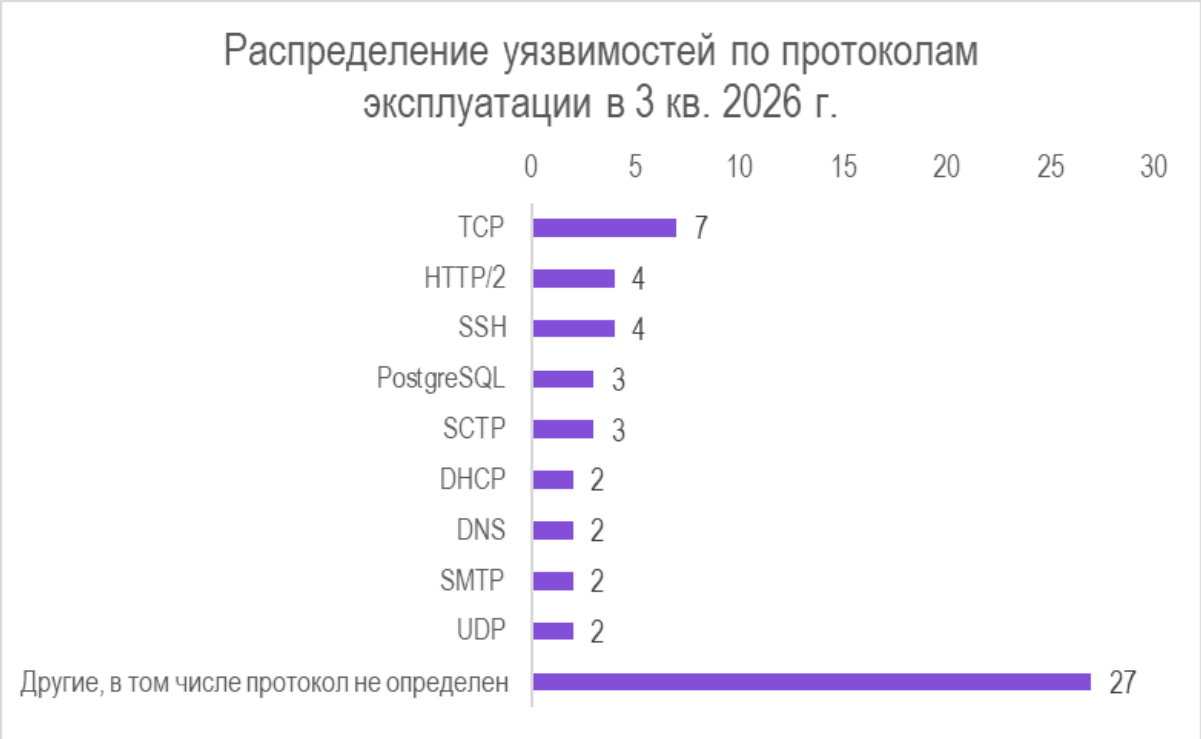
CVE-2026-54121 (8,8/10) — уязвимость в Active Directory Certificate Services (AD CS), позволяющая авторизованному атакующему повысить привилегии по сети (CWE: 285 — Improper Authorization).

CVE-2026-30623 (9,8/10) — критическая уязвимость Command Injection (CWE: 77) в LiteLLM, AI-платформе для работы с LLM. Через функцию создания MCP-сервера возможно выполнение произвольных команд на сервере.

CVE-2026-57850 (8,3/10) — уязвимость Missing Authorization (CWE: 862) в RustDesk, позволяющая аутентифицированному удаленному пользователю обойти ограничения сессии и выполнять действия за пределами предоставленных ему прав.

CVE-2026-33453 (10,0/10) — уязвимость Header Injection (CWE: 915) в компоненте camel-coap Apache Camel, позволяющая через специально сформированные CoAP-запросы внедрять camel-заголовки и при определенных конфигурациях выполнять произвольный код.

CVE-2026-40453 (9,9/10) — уязвимость Header Injection (CWE: 178) в Apache Camel, позволяющая обходить фильтрацию заголовков с помощью изменения регистра символов и потенциально добиться выполнения команд или записи произвольных файлов.



Протокол	Количество	Доля от CVE, %

TCP	7	6,5
HTTP/2	4	3,7
SSH	4	3,7
PostgreSQL	3	2,8
SCTP	3	2,8
DHCP	2	1,9
DNS	2	1,9
SMTP	2	1,9
UDP	2	1,9
Другие, в том числе протокол не определен	27	73
Итого	108	100,0

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

CVE	Количество	Описание
CVE-2026-54121	15	CVE-2026-54121 (8,8/10) — уязвимость в Active Directory Certificate Services (AD CS), позволяющая авторизованному атакующему повысить привилегии по сети
CVE-2026-67276	6	CVE-2026-67276 (9,2/10) — критическая уязвимость в MikroTik RouterOS, позволяющая неаутентифицированному атакующему по сети обойти проверку RSA-ключа при SSH-аутентификации и получить доступ к командному интерфейсу от имени авторизованного пользователя
CVE-2026-88772	6	CVE-2026-88772 (9,5/10) — критическая уязвимость в Citrix NetScaler ADC и

		NetScaler Gateway, связанная с переполнением буфера памяти при обработке DTLS
CVE-2026-86060	5	CVE-2026-86060 (9,8/10) — критическая уязвимость в MikroTik RouterOS, связанная с некорректной обработкой аргументов при SSH-аутентификации
CVE-2026-25243	4	CVE-2026-25243 (8,8/10) — уязвимость в Redis, связанная с некорректной проверкой сериализованных данных командой RESTORE

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

Общее количество таких уязвимостей составило 12. Средняя степень критичности по шкале CVSS — 7,9. В этом квартале не встретилось уязвимостей, эксплуатируемых по протоколу gRPC.

Распределение уязвимостей по протоколам эксплуатации:

Протокол	Количество	Доля от CVE, %
WebSocket	8	66,7
HTTP/2	4	33,3
gRPC	0	0
Итого	12	100

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

CVE-2026-34048 (9,9/10) — критическая уязвимость в Coolify, связанная с отсутствием проверки авторизации (CWE: 862) для WebSocket-маршрутов терминала. Пользователь с низкими привилегиями может подключиться к терминалу серверов команды и выполнять на них произвольные команды.

CVE-2026-15409 (10,0/10) — критическая уязвимость SSRF (CWE: 918) в интерфейсе WorkPlace SonicWall SMA1000. Неаутентифицированный удаленный атакующий может заставить устройство выполнять запросы к произвольным ресурсам, что потенциально

позволяет получить доступ к внутренним системам и чувствительным данным. Уязвимость включена в CISA KEV.

CVE-2026-56848 (7,5/10) — уязвимость Node.js в обработке HTTP/2, приводящая к Use-After-Free (CWE: 416) в памяти. Удаленный неаутентифицированный атакующий может вызвать аварийное завершение приложения и отказ в обслуживании.

CVE-2026-1961 (8/10) — уязвимость Command Injection (CWE: 78) в WebSocket-прокси Foreman. Злоумышленник, контролирующий сервер вычислительных ресурсов, может передать специально сформированное имя хоста и добиться выполнения команд на сервере Foreman при обращении пользователя к VNC-консоли виртуальной машины.

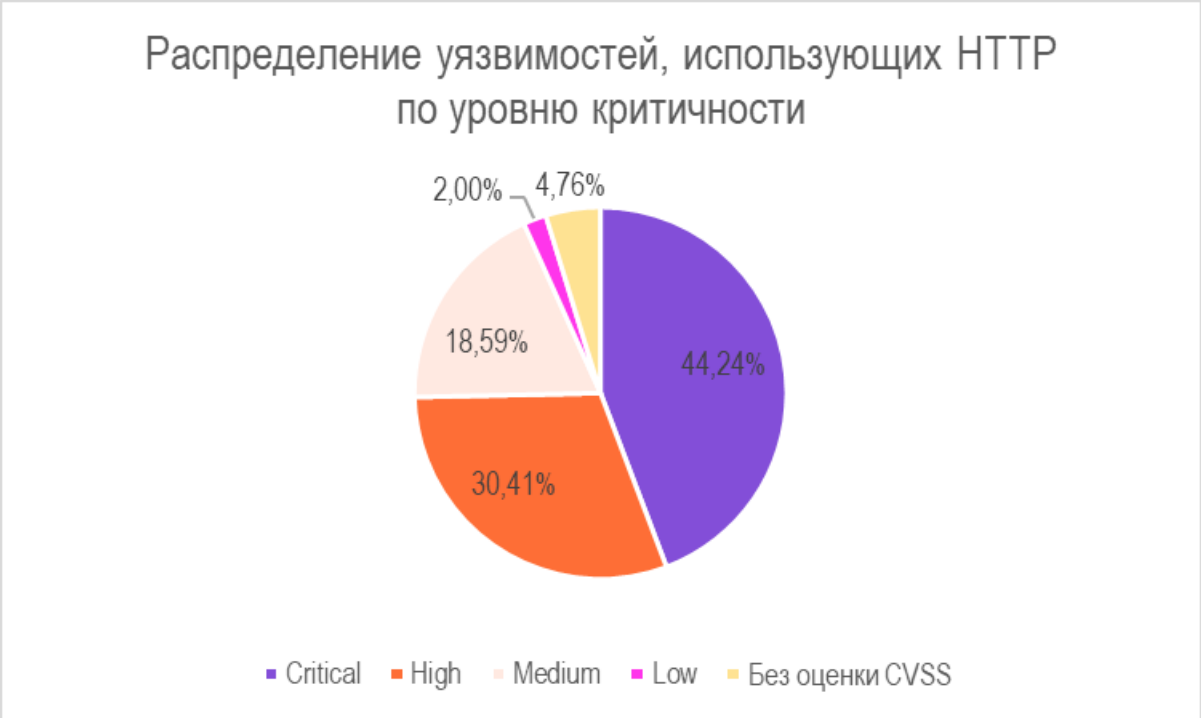
CVE-2026-86350 (6,5/10) — уязвимость Apache Tomcat в обработке HTTP/2, связанная с некорректной интерпретацией запросов (CWE: 444 — HTTP Request/Response Smuggling). Она может привести к смешению заголовков запросов и нарушению их обработки сервером.

Сетевые уязвимости, использующие протокол HTTP

В третьем квартале количество опубликованных сканеров, PoC и эксплойтов, использующих HTTP-протокол составило 652. Распределение уровней критичности за третий квартал 2026 года среди уязвимостей с использованием HTTP-протокола составило:

Уровни критичности (баллы)	
Максимальный	10
Минимальный	1,2
Средний	8,24
Медианный	8,8

73,52% всех уязвимостей имели критичный и высокий уровень опасности.



Десятибалльную оценку получили 37 уязвимостей.

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.

В третьем квартале большая часть таких уязвимостей была зафиксирована в популярных браузерах Firefox и Google Chrome. Часть из них перечислена ниже:

CVE-2026-6307 (8,8) — это уязвимость в Google Chrome, которая позволяет удаленному злоумышленнику выполнить произвольный код внутри песочницы браузера при открытии специально подготовленной HTML-страницы. Проблема

связана со смешением типов данных в компиляторе TurboFan движка V8. Исправлена в версии 147.0.7727.101.

CVE-2026-14431 (8,8) — это уязвимость в Google Chrome, которая позволяет удаленному злоумышленнику выполнить произвольный код внутри песочницы браузера через специально подготовленную HTML-страницу. Проблема связана со смешением типов данных в движке JavaScript V8. Исправлена в версии 150.0.7871.46.

CVE-2026-10702 (7,5) — это уязвимость в Mozilla Firefox, связанная с некорректной компиляцией JavaScript-кода компонентом JIT. Ошибка приводит к неправильной обработке кода и может нарушить работу браузера при обработке вредоносного содержимого. Исправлена в версии 151.0.3.

CVE-2026-2766 (9,8) — это уязвимость в Mozilla Firefox и Thunderbird, связанная с использованием памяти после ее освобождения (use-after-free) в JIT-компоненте движка JavaScript. Такая ошибка может привести к повреждению памяти, аварийному завершению приложения и потенциальному выполнению произвольного кода. Исправлена в Firefox 148, Firefox ESR 140.8, Thunderbird 148 и Thunderbird 140.8.

CVE-2026-2764 (9,8) — это уязвимость в Mozilla Firefox и Thunderbird, связанная с некорректной JIT-компиляцией JavaScript и использованием памяти после ее освобождения (use-after-free). Ошибка может привести к повреждению памяти и потенциальному выполнению произвольного кода. Исправлена в Firefox 148, Firefox ESR 115.33 и 140.8, Thunderbird 148 и 140.8.

CVE-2026-4692 (10,0) — это уязвимость в Mozilla Firefox и Thunderbird, которая позволяет выйти за пределы песочницы и обойти ограничения изоляции приложения. Проблема связана с компонентом Responsive Design Mode, предназначенным для проверки адаптивного отображения веб-страниц. Исправлена в Firefox 149, Firefox ESR 115.34 и 140.9, Thunderbird 149 и 140.9.

Общее количество уязвимостей в данных браузерах:
Firefox — 12;
Google Chrome — 11.
Средняя критичность всех уязвимостей имеет высокий уровень опасности. Так что, если вы давно не обновляли браузер, сейчас самое время.

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.
Наиболее интересные и наиболее критичные.

CVE-2026-100903 (5,3) — это уязвимость в GEOritm компании НПО «Ритм», которая позволяет удаленному злоумышленнику получить доступ к данным без аутентификации. Проблема связана с отсутствием проверки подлинности при

обработке параметра objectId в REST API /restapi/objects/obj-groups. Исправлена в версии 2.46.

CVE-2026-629111 (8,0) — это уязвимость в Microsoft Exchange Server, которая позволяет злоумышленнику с учетной записью повысить привилегии через сеть. Проблема связана с обходом аутентификации путем перехвата и повторного воспроизведения аутентификационных данных (capture-replay). Для эксплуатации требуется взаимодействие пользователя.

CVE-2026-9086 (7,3) — это XSS-уязвимость в Keycloak, которая позволяет выполнить вредоносный JavaScript в браузере пользователя в контексте Keycloak. Проблема связана с обходом проверки URI посредством изменения регистра символов в схемах javascript: и data:. Для эксплуатации необходимы права управления клиентами либо доступ к регистрации клиентов, а также переход жертвы по подготовленной ссылке.

CVE-2026-64638 (8,9) — это уязвимость отраженного межсайтового скриптинга (XSS) на странице входа WordPress, доступная для эксплуатации без аутентификации. При определенных условиях и активном взаимодействии жертвы атака может привести к выполнению PHP-кода на сервере. Исправлена в WordPress 7.0.3; исправления также выпущены для предыдущих веток вплоть до 4.7.

CVE-2026-75650 (10,0) — это уязвимость в Adobe Commerce, Adobe Commerce B2B и Magento Open Source, которая позволяет удаленному злоумышленнику выполнить произвольный код без аутентификации. Проблема связана с недостаточной нейтрализацией специальных элементов при обработке данных шаблонизатором, что делает возможной инъекцию в шаблоны.

CVE-2026-100382 (10,0) — это уязвимость в расширении ExternalData для MediaWiki, которая позволяет неаутентифицированному злоумышленнику выполнить команды операционной системы через специально подготовленный вики-текст. Проблема связана с недостаточной нейтрализацией специальных символов при формировании системных команд. Исправлена в ExternalData 3.7.

CVE-2026-85706 (10,0) — это уязвимость обхода каталогов (path traversal) в GitLab Community Edition и Enterprise Edition, которая при определенных условиях позволяет неаутентифицированному злоумышленнику читать произвольные файлы на сервере. Проблема связана с недостаточным ограничением файловых путей и отсутствием обязательной проверки аутентификации в API коммитов репозитория.

CVE-2026-50522 (9,8) — это уязвимость в Microsoft SharePoint Server, которая позволяет удаленному злоумышленнику выполнить произвольный код без аутентификации. Проблема связана с небезопасной десериализацией недоверенных данных, полученных через сеть. Затрагивает SharePoint Server 2016, 2019 и Subscription Edition.

CVE-2026-20896 (9,8) — это уязвимость в официальных docker-образах Gitea, которая позволяет выдать себя за другого пользователя, включая администратора, посредством поддельного HTTP-заголовка. Проблема связана с доверием ко всем IP-

адресам в настройке REVERSE_PROXY_TRUSTED_PROXIES. Эксплуатация возможна при включенной аутентификации через обратный прокси и прямом доступе к HTTP-порту контейнера. Исправлена в версии 1.26.3.

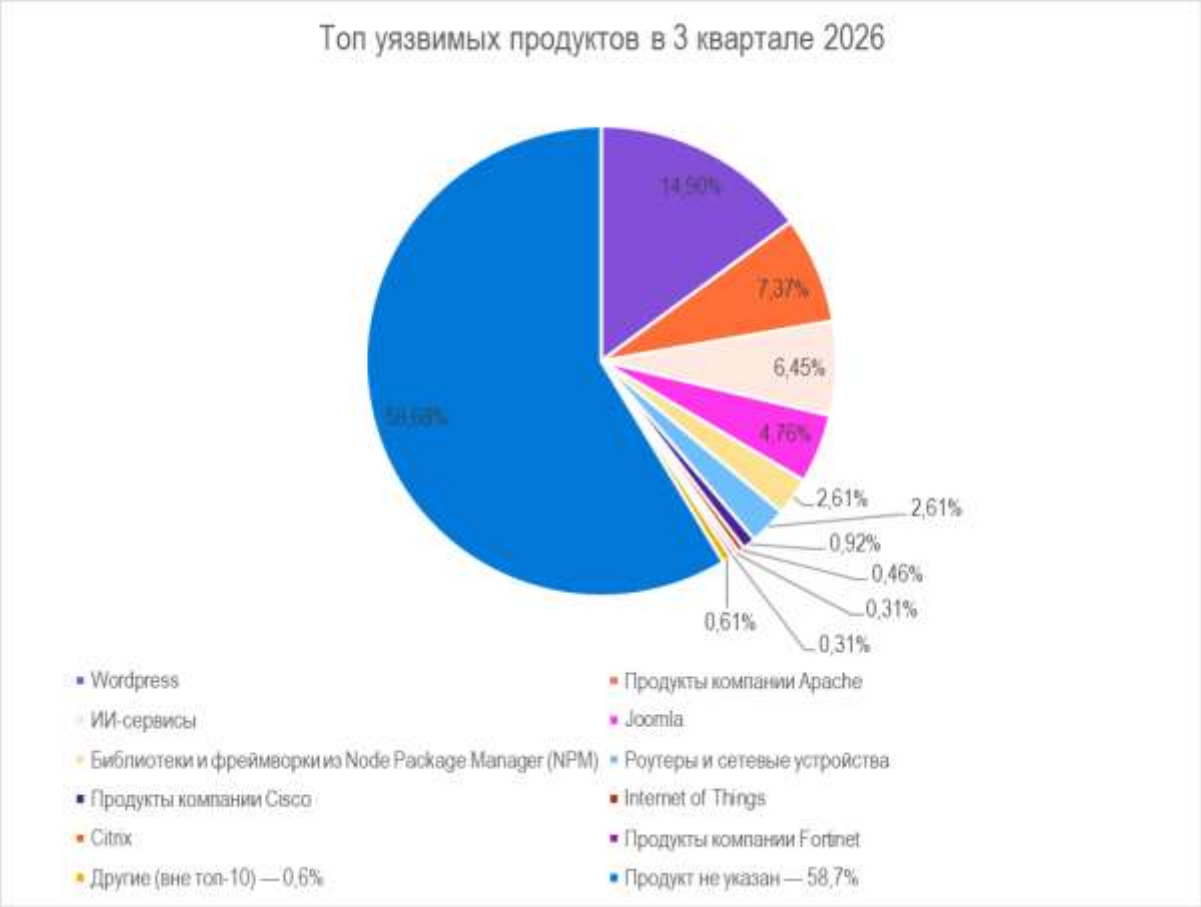
CVE-2026-41452 (9,8) — это уязвимость в Krayin CRM, которая позволяет неаутентифицированному злоумышленнику перезаписать данные основной учетной записи администратора и получить полный административный доступ. Проблема связана с отсутствием аутентификации в API установщика и возможностью обойти проверку, запрещающую повторную настройку уже установленной системы.

Уязвимости в продуктах, эксплуатируемых по протоколу HTTP

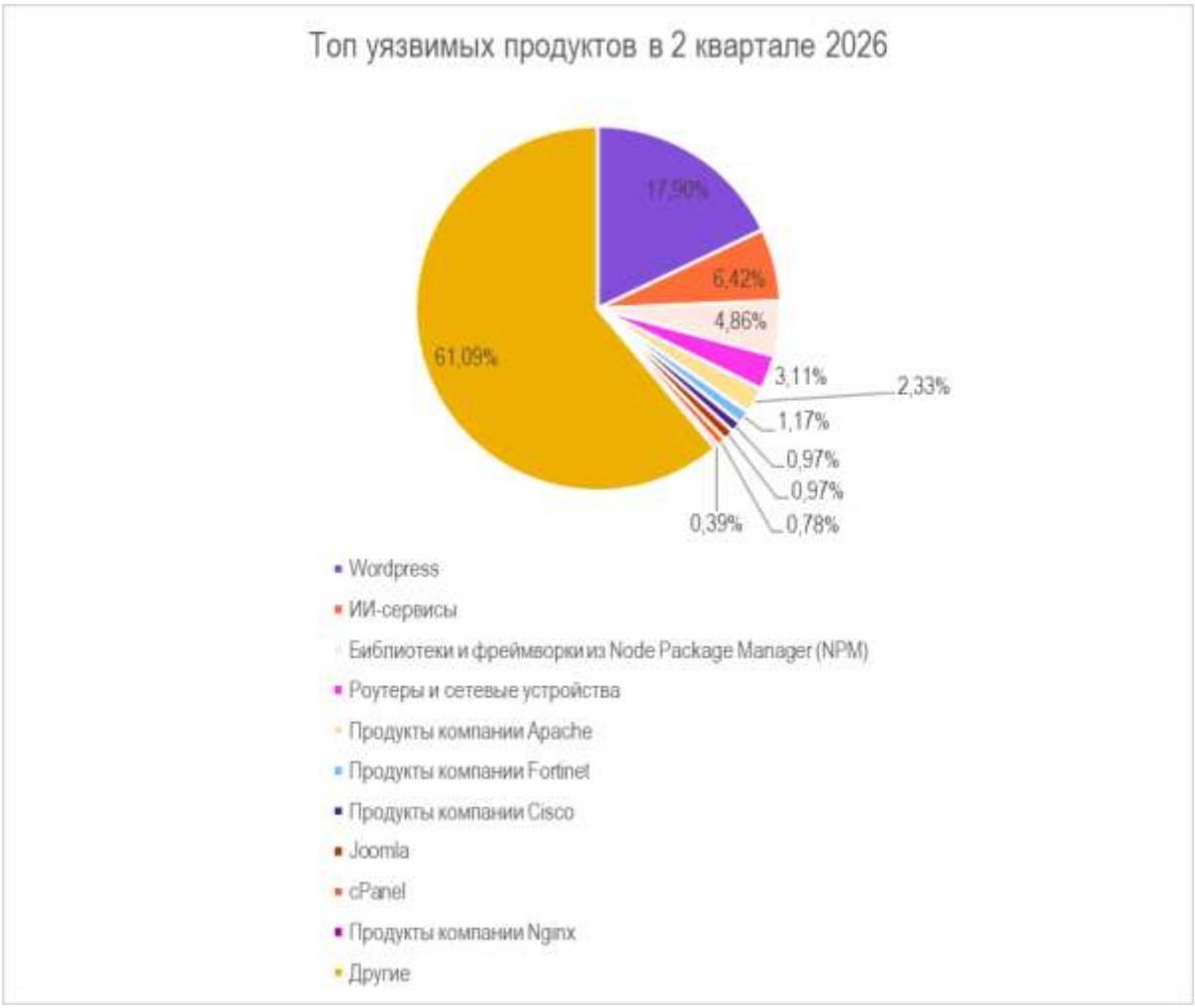
Данный раздел посвящен уязвимостям, которые могут эксплуатироваться злоумышленником из внешней сети интернет. Ниже продемонстрирована таблица для наиболее критичных сервисов, вендоров и продуктов, в данном квартале мы выделили:

Продукт	**Количество уязвимостей в 2 кв.**	**Количество уязвимостей в 3 кв.**
WordPress	92	97
AI-сервисы	33	44
Библиотеки и фреймворки из Node Package Manager (npm)	25	18
Роутеры и сетевые устройства	16	26
Продукты компании Apache	12	69
Продукты компании Fortinet	6	2
Продукты компании Cisco	5	5
Joomla	5	32
cPanel	4	3
Продукты компании Nginx	2	1
Microsoft Office SharePoint	1	4
Другие	314	

В третьем квартале значительно выросла доля уязвимостей в продуктах компании Apache. Но стоит отметить, что большая часть PoC-демонстраций представляют собой лабораторные стенды с автоматической демонстрацией уязвимости для Apache Camel. Это не значит, что злоумышленник не сможет, основываясь на этих данных, собрать собственный эксплойт. Поэтому, если вы используете Apache Camel, настоятельно рекомендуем обновиться. Уязвимости в CMS Joomla также показали значительный рост в количестве вышедших PoC. Если раньше мы часто акцентировали внимание об уязвимости в плагинах WordPress, то третий квартал принес уязвимости и самого ядра WordPress.



В предыдущем квартале топ выглядел следующим образом:


Топ уязвимых продуктов в 2 квартале 2026
17,90%
6,42%
4,86%
3,11%
2,33%
1,17%
0,97%
0,97%
0,78%
0,39%
61,09%
Wordpress
ИИ-сервисы
Библиотеки и фреймворки из Node Package Manager (NPM)
Роутеры и сетевые устройства
Продукты компании Apache
Продукты компании Fortinet
Продукты компании Cisco
Joomla
cPanel
Продукты компании Nginx
Другие

Content Management Systems

Данный раздел посвящен уязвимостям в CMS-платформах, которые удалось обнаружить в третьем 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 других CMS, например Joomla, Concrete и т. д.

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

Количество CVE	97
Средний CVSS	8,49
Min CVSS	3,7
Max CVSS	10
Самая популярная CWE	CWE-434
Максимально критичная CVE (CVSS: 10)	CVE-2026-57811, CVE-2026-77770, CVE-2026-81648, CVE-2026-82222

WordPress
Как мы уже отмечали, третий квартал принес громкие уязвимости ядра WordPress. Данные уязвимости получили собственные названия:

Click2Shell (7,1) — это цепочка уязвимостей WordPress, которая позволяет выполнить PHP-код на сервере после перехода авторизованного администратора по специально подготовленной ссылке. Инъекция в jQuery-селектор механизма предпросмотра вызывает установку выбранной злоумышленником темы из каталога WordPress.org, а отдельная уязвимость этой темы обеспечивает выполнение кода. Ошибка ядра исправлена в WordPress 7.1.1. В публикации исследователей CVE пока не указан; оценка 7,1 относится к принудительной установке темы.

Wp2shell — CVE-2026-63030 и CVE-2026-60137 (9,1) — это цепочка уязвимостей ядра WordPress, которая позволяет неаутентифицированному злоумышленнику выполнить произвольный код на сервере без участия пользователя. Проблема связана с ошибкой сопоставления маршрутов пакетных запросов REST API и SQL-инъекцией в параметре author__not_in компонента WP_Query. Для эксплуатации не требуются дополнительные плагины или темы. Цепочка исправлена в WordPress 6.9.5 и 7.0.2.

Comment2Shell — CVE-2026-93485 (7,1) — это уязвимость хранимого межсайтового скриптинга (XSS) в WordPress, которая позволяет внедрить вредоносный JavaScript через анонимный комментарий. Проблема связана с некорректным преобразованием HTML функцией wpautop() при отображении комментариев в определенных темах. Если страницу откроет авторизованный администратор с правом установки плагинов, выполнение скрипта может привести к выполнению PHP-кода на сервере. Исправлена в WordPress 7.1.1.
Но и помимо уязвимостей ядра, также были опубликованы PoC/exploit в популярных плагинах, например:

CVE-2026-15748 (9,8) — это уязвимость в плагине Furminator Forms для WordPress,

которая позволяет неаутентифицированному злоумышленнику загружать произвольные файлы, включая PHP-код. Проблема связана с недостаточной проверкой типов файлов и доверием к поддельной конфигурации полей формы. Для эксплуатации требуется форма с полями File Upload и Select; выполнение кода возможно, если каталог загрузки допускает запуск PHP. Исправлена в версии 1.56.2.

CVE-2026-82222 (10,0) — это уязвимость в плагине GiveWP для WordPress, которая при определенных настройках форм пожертвований и регистрации позволяет злоумышленнику без предварительной учетной записи выполнить произвольный код на сервере. Проблема связана с небезопасной десериализацией данных, позволяющей внедрять PHP-объекты и использовать цепочку методов встроенных классов для выполнения системных команд. Исправлена в версии 4.16.7.2.

Joomla

В CMS Joomla был зафиксирован всплеск количества вышедших PoC/exploit. Существенную часть всех уязвимостей занимают ошибки в валидации JavaScript-кода (XSS) и SQL-кода (SQLi). Кратко опишем наиболее критичные уязвимости:

CVE-2026-56290 (10,0) — это уязвимость в расширении Page Builder CK для Joomla, которая позволяет неаутентифицированному злоумышленнику загрузить исполняемый PHP-файл и выполнить код на сервере. Проблема связана с отсутствием проверки прав доступа в обработчике загрузки файлов. Первоначальное исправление выпущено в версии 3.6.0; последующие связанные проблемы устранены в версии 3.6.5.

CVE-2026-57827 (10,0) — это уязвимость в расширении RSFiles! для Joomla, которая позволяет неаутентифицированному злоумышленнику загрузить произвольный файл и выполнить PHP-код на сервере. Проблема связана с возможностью напрямую вызвать обработчик записи файла, обходя проверки прав доступа и допустимых расширений. Исправлена в версии 1.17.12.

CVE-2026-65883 (10,0) — это уязвимость в плагине Aimy Captcha-Less Form Guard для Joomla, которая позволяет неаутентифицированному злоумышленнику внедрить PHP-объекты через поддельное поле формы clfgd. Проблема связана с небезопасной десериализацией недоверенных данных и, при наличии подходящей цепочки методов загруженных классов, приводит к выполнению кода на сервере. Затрагивает версии 18.0–20.0, исправлена в 20.1.

CVE-2026-61424 (10,0) — это уязвимость в расширении DJ-Classifieds для Joomla, которая позволяет неаутентифицированному злоумышленнику загружать файлы с вредоносным содержимым. Проблема связана с отсутствием проверки доступа и недостаточной фильтрацией файлов в обработчике загрузки изображений. Выполнение кода возможно при соответствующей конфигурации сервера либо в сочетании с уязвимостью включения локальных файлов. Исправлена в версии 3.11.2.

CVE-2026-77991 (9,4) — это уязвимость в расширении Joomla Event Manager (JEM), которая позволяет пользователю с административными правами записать исполняемый PHP-файл и выполнить код на сервере. Проблема связана с отсутствием ограничения опасных типов файлов в компоненте работы с исходными файлами административной панели. Затрагивает версии ниже 5.0.1.

CVE-2026-97163 (10,0) — это уязвимость в расширении UP Universal Plugin для Joomla, которая позволяет неаутентифицированному злоумышленнику инициировать загрузку и установку программного кода через AJAX-интерфейс. Проблема связана с

недостаточным контролем доступа к механизму установки дополнительных действий; загрузка кода также выполняется без проверки TLS-сертификатов. Затрагивает версии 5.0.0–5.2.0 и 6.0.0–6.0.29, исправлена в 5.2.1 и 6.1.

Craft CMS

CVE-2026-31857 (8,8) — это уязвимость в Craft CMS, которая позволяет авторизованному пользователю панели управления, включая автора или редактора, выполнить произвольный код на сервере. Проблема связана с обработкой пользовательских условий фильтрации через шаблонизатор Twig без изоляции и экранирования.

CVE-2026-28695 (7,2) — это уязвимость в Craft CMS, которая позволяет пользователю с административными правами или доступом к инструменту System Messages выполнить произвольные команды на сервере. Проблема связана с внедрением кода в шаблоны Twig: функция create() позволяет создавать PHP-объекты и использовать компонент Symfony Process для выполнения команд.

CVE-2026-44011 (8,6) — это уязвимость в Craft CMS, которая позволяет авторизованному пользователю выполнить произвольные команды на сервере. Проблема связана с недостаточной проверкой конфигурации при создании объектов Yii: специально подготовленные данные позволяют подключить вредоносный компонент Behavior и запустить его при инициализации объекта.

Concrete CMS

CVE-2026-93659 (9,3) — это уязвимость хранимого межсайтового скриптинга (XSS) в дополнении Community Store для Concrete CMS до версии 2.7.8. Проблема связана с отсутствием HTML-экранирования полей заказа, включая имя, email и телефон покупателя. Внедренный скрипт выполняется в браузере менеджера при просмотре заказа и позволяет создавать несанкционированные учетные записи или похищать данные.

CVE-2026-8239 (6,3) — это уязвимость контроля доступа (IDOR) в Concrete CMS версии 9.5.0 и ниже, которая позволяет неаутентифицированному злоумышленнику узнавать о существовании сообщений и получать их рейтинг. Проблема связана с отсутствием проверки прав доступа в обработчике /ccm/frontend/conversations/get_rating, принимающем идентификатор сообщения.

CVE-2026-8237 (6,3) — это уязвимость контроля доступа (IDOR) в Concrete CMS версии 9.5.0 и ниже, которая позволяет неаутентифицированному злоумышленнику читать сообщения из закрытых разделов и очереди модерации, а также получать сведения о вложениях и ссылки на их скачивание. Проблема связана с отсутствием проверки прав доступа в обработчике /ccm/frontend/conversations/message_detail.

XenForo

CVE-2026-73312 (9,1) — это уязвимость в XenForo до версии 2.3.13, которая позволяет атакующему, получившему токен обновления OAuth2, многократно использовать его для получения новых пар токенов. Проблема связана с тем, что после истечения срока действия связанного токена доступа токен обновления не помечается как использованный, позволяя сохранять несанкционированный доступ в течение срока его действия.

CVE-2026-73311 (9,1) — это уязвимость в XenForo до версии 2.3.13, которая позволяет повторно использовать код авторизации OAuth2 для получения дополнительных пар токенов от имени пользователя. Проблема связана с отсутствием аннулирования кода после первоначального обмена на токены, что нарушает требование его однократного использования.

CVE-2026-73309 (9,1) — это уязвимость обхода аутентификации OAuth2 в XenForo до версии 2.3.13, которая позволяет атакующему с действительным кодом авторизации получить токены без подтверждения подлинности клиента и проверки PKCE. Проблема связана с некорректной обработкой пустых значений `client_secret` и `code_verifier`, из-за которой соответствующие проверки пропускаются.

CVE-2026-73316 (8,7) — это уязвимость в интеграции PayPal REST в XenForo до версии 2.3.13, которая позволяет повторно обрабатывать одно и то же уведомление об оплате, вызывая повторную активацию подписок и неправомерное предоставление платных возможностей. Проблема связана с отсутствием проверки повторяющихся идентификаторов транзакций при обработке webhook-уведомлений.

AI-сервисы и агенты

В третьем квартале было обнаружено множество уязвимостей в различных AI-инструментах. Лидером по количеству найденных уязвимостей Langflow за квартал опубликовано 18 PoC/exploit-репозиториев.

Количество CVE	46
Средний CVSS	8,83
Min CVSS	2,3
Max CVSS	10
Самая популярная CWE	CWE-94
Максимально критичная CVE (CVSS: 10)	CVE-2026-10134, CVE-2026-26216, CVE-2026-42298, CVE-2026-54350, CVE-2026-59726, CVE-2026-66012, CVE-2026-73678

CVE-2026-55255 (8,4) — это уязвимость контроля доступа (IDOR) в Langflow до версии 1.9.1, которая позволяет авторизованному злоумышленнику запускать рабочие процессы других пользователей, получать обрабатываемые ими данные и расходовать их ресурсы. Проблема связана с отсутствием проверки владельца процесса при обращении по его UUID через `/api/v1/responses`.

CVE-2026-27966 (9,8) — это уязвимость в компоненте CSV Agent платформы Langflow, которая позволяет выполнить произвольный python-код и системные команды через

внедрение инструкций в запрос к языковой модели. Проблема связана с принудительно включенной настройкой `allow_dangerous_code=True`, предоставляющей агенту доступ к исполнению python-кода на сервере.

CVE-2026-54350 (9,8) — это уязвимость внедрения NoSQL-операторов в Budibase, которая позволяет неаутентифицированному посетителю опубликованного приложения читать документы подключенной коллекции, а при наличии публичного запроса записи — массово изменять их. Проблема связана с подстановкой пользовательских параметров в JSON-шаблоны запросов без необходимого экранирования.

CVE-2026-27495 (9,9) — это уязвимость выхода из песочницы JavaScript Task Runner в n8n, которая позволяет авторизованному пользователю с правом создания или изменения рабочих процессов выполнить произвольный код за пределами изолированной среды. При включенных внутренних Task Runners эксплуатация может привести к полной компрометации сервера n8n.

CVE-2026-26216 (10,0) — это уязвимость в Docker API платформы Crawl4AI до версии 0.8.0, которая позволяет неаутентифицированному злоумышленнику выполнить произвольные системные команды. Проблема связана с исполнением python-кода из параметра `hooks` обработчика `/crawl` и разрешенным импортом произвольных модулей через `__import__`.

CVE-2026-59726 (10,0) — это уязвимость в Ruflo до версии 3.16.3, которая позволяет неаутентифицированному злоумышленнику выполнять команды в контейнере MCP bridge и похищать ключи API. Проблема связана с отсутствием аутентификации на MCP-обработчиках в стандартном развертывании Docker Compose и возможностью вызова инструмента `terminal_execute` в обход ограничений.

CVE-2026-12940 (9,8) — это уязвимость в Langflow OSS, которая позволяет неаутентифицированному злоумышленнику выполнить произвольный код через внедрение переменных окружения при запуске MCP-сервера в режиме stdio. Проблема связана с неполным списком запрещенных переменных, в котором отсутствуют `SHELLOPTS`, `BASHOPTS` и `PS4`.

CVE-2026-24770 (9,8) — это уязвимость Zip Slip в компоненте MinerUParser платформы RAGFlow, которая позволяет перезаписывать файлы на сервере и впоследствии выполнять произвольный код. Проблема связана с отсутствием проверки путей внутри ZIP-архива, получаемого от внешнего сервиса MinerU, при его распаковке.

CVE-2026-64849 (9,3) — это уязвимость подделки серверных запросов (SSRF) в механизме вебхуков MLflow, которая позволяет обращаться к внутренним сервисам и облачным службам метаданных, получая содержимое ответов. Проблема связана с проверкой только исходного URL без повторной проверки перенаправлений и защиты от подмены DNS-адреса; стандартное развертывание допускает эксплуатацию без аутентификации.

CVE-2026-47851 (7,5) — это уязвимость отказа в обслуживании в компоненте PDF Document Reader платформы Spring AI. Проблема связана с неограниченной рекурсией при обработке PDF с глубоко вложенным или циклическим оглавлением, что вызывает переполнение стека и аварийное завершение потока обработки документа.

Уязвимости в пакетах NPM (Node Package Manager)

Количество CVE	18
Средний CVSS	8,31
Min CVSS	5,3
Max CVSS	9,5
Самая популярная CWE	CWE-22
Максимально критичная CVE (CVSS: 9.5)	CVE-2026-100721

CVE-2026-75604 (9,0) — это уязвимость в Next.js, которая позволяет неаутентифицированному злоумышленнику выполнить произвольный код на сервере под Windows. Проблема связана с обходом ограничений файловых путей и затрагивает приложения, использующие Pages Router или App Router без Cache Components.

CVE-2026-44351 (9,1) — это уязвимость в библиотеке fast-jwt до версии 6.2.4, которая позволяет подделывать JWT-токены и обходить аутентификацию. Проблема возникает, когда асинхронная функция получения ключа возвращает пустую строку или буфер нулевой длины: при разрешенных алгоритмах HMAC библиотека принимает пустой секретный ключ и признает поддельную подпись действительной.

CVE-2026-29057 (6,3) — это уязвимость контрабанды HTTP-запросов (HTTP Request Smuggling) в Next.js при проксировании запросов на внешний сервер через правила rewrites. Проблема связана с различной интерпретацией границ запроса прокси-сервером и бэкендом, что позволяет внедрить дополнительный запрос к внутренним или административным маршрутам.

CVE-2026-100721 (9,5) — это уязвимость в библиотеке vm2 до версии 3.12.2, которая позволяет выйти из песочницы и выполнить произвольный код в основном процессе приложения. Проблема связана с некорректной проверкой путей внешних модулей в NodeVM при использовании пользовательского механизма разрешения модулей и настройки `context: 'host'`: совпадение начала пути позволяет загрузить модуль, отсутствующий в списке разрешенных.

CVE-2026-45746 (9,0) — это уязвимость контроля доступа в файловом менеджере Termix до версии 2.3.2, которая позволяет авторизованному злоумышленнику

использовать активные сеансы других пользователей для доступа к файлам и выполнения команд на их удаленных серверах. Проблема связана с отсутствием проверки принадлежности переданного параметра `sessionId` текущему пользователю.

CVE-2026-45750 (9,0) — это уязвимость внедрения команд в файловом менеджере Termix, которая позволяет авторизованному пользователю выполнить произвольные команды на удаленном сервере через активное SSH-соединение. Проблема связана с недостаточным экранированием параметра `path` в обработчике `resolvePath` перед его включением в команду оболочки. Исправлена в версии 2.3.2.

CVE-2026-53547 (8,8) — это уязвимость в Termix до версии 2.3.2, которая позволяет авторизованному пользователю с низкими привилегиями захватить чужую локальную учетную запись, включая административную. Проблема связана с включением глобальной таблицы настроек в пользовательский экспорт базы данных: содержащиеся в ней коды и временные токены сброса пароля позволяют изменить пароль другого пользователя.

Уязвимости в роутерах и другом сетевом оборудовании

Количество CVE	26
Средний CVSS	8,49
Min CVSS	6,5
Max CVSS	9,8
Самая популярная CWE	CWE-77
Максимально критичная CVE (CVSS: 9.8)	CVE-2026-58457

CVE-2026-93958 (9,1) — это уязвимость внедрения команд в D-Link R95 с прошивкой BE9500_1.00.16, которая позволяет удаленному злоумышленнику с высокими привилегиями выполнить произвольные системные команды. Проблема связана с недостаточной проверкой параметра `NTPServer` в компоненте DHMAPI перед передачей данных функции `system` в `/bin/ssi`.

CVE-2026-82592 (9,9) — это уязвимость переполнения буфера стека в D-Link DIR-825M с прошивкой 1.1.8, которая позволяет авторизованному злоумышленнику вызвать отказ в обслуживании или выполнить произвольный код. Проблема связана с отсутствием проверки длины параметра `partition` в обработчике форматирования диска `/boafrm/formDiskFormat`.

Уязвимости в Apache и Nginx

Количество CVE	69
Средний CVSS	7,84
Min CVSS	3,7
Max CVSS	10
Самая популярная CWE	CWE-20
Максимально критичная CVE (CVSS: 9,8)	CVE-2026-47323

Apache Camel собрал большое количество уязвимостей в третьем квартале 2026 года. Для всех них существуют PoC это именно PoC, а не эксплойты. Концепции представляют из себя лабораторные стенды, которые выглядят похожим образом
CVE-2026-40453/
├── pom.xml
├── Dockerfile
├── docker-compose.yml

```
├── README.md
└── src/main/
 ├── java/com/example/
 │  ├── Application.java
 │  ├── CoapExecRoute.java # victim: from(coap).to(exec)
 │  └── ExploitController.java # /normal, /canonical (filtered), /attack (case-variant bypass)
 └── resources/
 └── application.properties
```

Данное описание взято из открытого репозитория CVE-2026-40453. Ниже приведем примеры уязвимостей, для которых есть полноценные скрипты, которые могут либо проверить уязвимость, либо эксплуатировать ее.

CVE-2026-82384 (9,8) — это уязвимость небезопасной десериализации в Apache Roller 6.1.5, которая позволяет неаутентифицированному злоумышленнику выполнить произвольный код на сервере. Проблема связана с обработкой специальных типов данных XML-RPC до проверки аутентификации, даже когда функция XML-RPC отключена в настройках.

CVE-2026-28672 (9,8) — это уязвимость внедрения системных команд в Apache Ranger версий 0.6–2.8. Проблема связана с недостаточной проверкой имени пользователя в компоненте `UnixUserGroupBuilder`, что позволяет внедрить произвольные команды при обработке пользователей и групп Unix.

CVE-2026-41042 (9,1) — это уязвимость в Apache Gravitino до версии 1.2.1, которая позволяет неаутентифицированному злоумышленнику выполнить произвольный java-код на сервере при использовании H2. Проблема связана с недостаточной проверкой JDBC URL в API `testConnection`, позволяющей передать опасный параметр `INIT`.

CVE-2026-59243 (9,8) — это уязвимость обхода аутентификации в Apache Airflow FAB provider до версии 3.7.3 при входе через Azure AD OAuth. Проблема связана с отключенной по умолчанию проверкой подписи JWT: поддельный или неподписанный ID-токен позволяет войти от имени другого пользователя, включая администратора.

CVE-2026-52680 (9,8) — это уязвимость обхода каталогов в Apache Kyuubi версий 1.7.0–1.11.1, которая позволяет злоумышленнику с доступом к REST API загрузки файлов записывать произвольное содержимое за пределами предназначенного каталога. Проблема связана с недостаточной проверкой переданного клиентом имени файла; возможности записи ограничены правами серверного процесса.

CVE-2026-44825 (8,1) — это уязвимость в Apache Solr версий 9.4.0–9.10.1 и 10.0.0, которая позволяет получить административный доступ к кластеру с помощью общеизвестных учетных данных. Проблема связана с тем, что команда `bin/solr auth enable` при включении BasicAuth незаметно создает дополнительные шаблонные учетные записи с фиксированными паролями.

Для nginx подобных уязвимостей нами зафиксировано не было.

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

Для Cisco в третьем квартале вышло 6 уязвимостей, но представляют они из себя не полноценные сканеры, PoC или эксплойты. А скорее попытки моделирования угрозы или сканирования эндпойнтов с перечислением разных полезных нагрузок для проверки валидации входных значений. Но для статистики мы учли эти уязвимости.

	cisco	citrix	fortinet
Количество CVE	6	3	2
Средний CVSS	9,02	9,2	8,85
Min CVSS	6,4	8,8	8,1
Max CVSS	10	9,5	9,6
Самая популярная CWE	CWE-20	CWE-119	CWE-1021
Максимально критичная CVE	CVE-2026-76460	CVE-2026-88772	CVE-2026-84388

CVE-2025-24472 (8,1) — это уязвимость обхода аутентификации в Fortinet FortiOS и FortiProxy, которая позволяет удаленному атакующему получить права суперадминистратора на подчиненном устройстве через специально сформированные CSF-запросы. Для эксплуатации необходима включенная функция Security Fabric и знание серийных номеров вышестоящего и подчиненного устройств.

CVE-2026-19490 (9,3) — это уязвимость в NetScaler ADC и NetScaler Gateway, которая позволяет удаленному атакующему обойти аутентификацию через альтернативный путь обработки запросов. Проблема затрагивает устройства, настроенные как Gateway или виртуальный сервер AAA; для некоторых версий дополнительно требуется настроенная SAML-аутентификация.

CVE-2026-8452 (8,8) — это уязвимость переполнения памяти в NetScaler ADC и NetScaler Gateway, которая позволяет удаленному атакующему без аутентификации вызвать некорректную работу устройства и отказ в обслуживании. Проблема проявляется при настройке устройства как Gateway (SSL VPN, ICA Proxy, CVPN, RDP Proxy) или виртуального сервера AAA.

CVE-2026-8451 (8,8) — это уязвимость чтения за пределами буфера в NetScaler ADC и NetScaler Gateway, которая может привести к раскрытию данных из памяти. Проблема связана с недостаточной проверкой входных данных и затрагивает устройства, настроенные как поставщик удостоверений SAML (SAML IdP).

Статистика CWE

В данном квартале вышел такой топ-10 CWE по отношению ко всем уязвимостям, которые эксплуатируются по протоколу HTTP.

CWE	Количество
CWE-79 (8.8%)	57
CWE-94 (8%)	52
CWE-22 (7,1%)	46
CWE-89 (6,9%)	45
CWE-434 (5,2%)	34



CWE-79
Помимо XSS-уязвимостей, для WordPress характерны сразу 4 уязвимости в MediaWiki.

CVE-2026-96875 (6,9) — это уязвимость межсайтового скриптинга (XSS) в расширении Cargo для MediaWiki до версии 3.9.4 включительно. Проблема связана с недостаточным экранированием данных в иерархических фильтрах Cargo Drilldown, что позволяет выполнить JavaScript в браузере пользователя в контексте сайта.

CVE-2026-96873 (5,5) — это уязвимость отраженного межсайтового скриптинга (XSS) в расширении CirrusSearch для MediaWiki до версии 1.46.0 включительно. Проблема связана с недостаточным экранированием данных в отладочном выводе объяснения результатов поиска, что позволяет внедрить JavaScript, выполняемый в браузере пользователя.

CVE-2026-96878 (6,9) — это уязвимость межсайтового скриптинга (XSS) в расширении Cargo для MediaWiki до версии 3.9.4 включительно. Проблема связана с недостаточным экранированием псевдонимов полей в формате отображения Exhibit, что позволяет внедрить JavaScript в формируемую страницу и выполнить его в браузере пользователя.

CVE-2026-96877 (6,9) — это уязвимость отраженного межсайтового скриптинга (XSS) в расширении Cargo для MediaWiki до версии 3.9.4 включительно. Проблема связана с недостаточным экранированием данных полнотекстового поиска в Cargo Drilldown, что позволяет выполнить внедренный JavaScript в браузере пользователя при открытии специально сформированной ссылки.

CWE-94

CVE-2026-84645 (8,8) — это уязвимость в Jenkins, которая позволяет атакующему с ограниченными правами выполнить произвольный код на сервере. Проблема связана с небезопасной десериализацией вложенных объектов в пользовательских файлах `config.xml`, позволяющей получить доступ к недостаточно защищенной Script Console через механизм обработки HTTP-запросов Stapler.

CVE-2026-58025 (5,9) — это уязвимость в MediaWiki, которая позволяет пользователю с высокими привилегиями выполнить произвольный код на сервере при импорте записей журнала. Проблема связана с небезопасной десериализацией недоверенных данных в компонентах импорта и обработки журналов.

CVE-2026-60004 (9,8) — это уязвимость в Gitea до версии 1.27.1, которая позволяет выполнить произвольные команды с правами системной учетной записи Gitea. Проблема связана с возможностью установки и запуска git-хуков через API `diffpatch`. Для эксплуатации требуется право записи в репозиторий; при открытой регистрации атакующий может получить его, создав собственную учетную запись и репозиторий.

CVE-2026-10134 (10,0) — это уязвимость в Langflow OSS версий 1.0.0–1.9.3, которая позволяет удаленному атакующему выполнить произвольный python-код на сервере. Проблема связана с передачей контролируемого атакующим кода в функцию `exec()` компонента PythonCodeStructuredTool. При наличии публичного потока с этим компонентом эксплуатация возможна без аутентификации и может привести к раскрытию секретов и изменению данных приложения.

CWE-22

CVE-2026-10053 (8,5) — это уязвимость обхода каталогов в реестре пакетов GitLab CE/EE, которая при определенных условиях позволяет аутентифицированному пользователю выполнить произвольный код на сервере. Проблема связана с недостаточной проверкой путей при обработке пакетов. Исправления выпущены в версиях 19.0.6, 19.1.4 и 19.2.2.

CVE-2026-48282 (10,0) — это уязвимость в Adobe ColdFusion, которая позволяет удаленному атакующему без аутентификации выполнить произвольный код на сервере. Проблема связана с недостаточным ограничением файловых путей, допускающим выход за пределы разрешенного каталога. Затронуты ColdFusion 2025 Update 9, ColdFusion 2023 Update 20 и более ранние обновления соответствующих веток.

CVE-2026-59774 (9,8) — это уязвимость в Gitea, которая позволяет удаленному атакующему без аутентификации читать файлы сервера через обработчик разметки публичного репозитория. Проблема связана с небезопасной обработкой директивы `#+INCLUDE` формата Org-mode. Раскрытие конфигурации и внутренних токенов может привести к выполнению произвольного кода с правами службы Gitea.

CWE-89

CVE-2026-25993 (9,3) — это уязвимость SQL-инъекции второго порядка в EverShop до версии 2.1.1, которая позволяет выполнять посторонние SQL-команды при обновлении или удалении категорий. Проблема связана с включением ранее сохраненного значения `url_key` в SQL-запросы посредством конкатенации строк без безопасной параметризации.

CVE-2026-52887 (10,0) — это уязвимость SQL-инъекции в NocoBase до версии 2.0.61, которая позволяет пользователю с обычной учетной записью читать данные базы и при стандартной конфигурации PostgreSQL выполнять команды внутри контейнера базы данных. Проблема связана с небезопасной обработкой фильтра в API `myInAppChannels:list`. При открытой регистрации атакующий может самостоятельно создать необходимую учетную запись.

CVE-2026-58048 (9,4) — это уязвимость повышения привилегий в cPanel & WHM и WP Squared, которая позволяет аутентифицированному пользователю с доступом к управлению MySQL/MariaDB выполнять SQL-команды с правами администратора базы данных. Проблема связана с некорректным сохранением режима SQL при переименовании баз; в зависимости от конфигурации возможна дальнейшая компрометация операционной системы.

CVE-2026-67689 (9,8) — это уязвимость SQL-инъекции в FineAdmin 1.0, которая позволяет удаленному атакующему внедрять SQL-команды через параметры `field` и `order` в запросах списков с постраничным выводом. Проблема связана с небезопасным формированием выражения сортировки `ORDER BY` и, согласно описанию CVE, может привести к выполнению произвольного кода.

CVE-2026-67401 (9,9) — это уязвимость SQL-инъекции в компоненте EmailTrack панели cPanel, которая позволяет аутентифицированному пользователю с почтовыми привилегиями создавать произвольные файлы на сервере. Успешная эксплуатация приводит к выполнению кода с правами root и полному контролю над сервером.

CWE-434
Большинство уязвимостей данного типа принадлежит к уязвимостям плагинов для CMS WordPress.

CVE-2026-87796 (9,8) — это уязвимость в плагине Multi Uploader for Gravity Forms для WordPress до версии 1.1.9 включительно, которая позволяет атакующему без аутентификации загружать произвольные файлы на сервер, что может привести к выполнению кода. Проблема связана с недостаточной проверкой типов файлов при обработке загрузки по частям.

CVE-2026-18351 (9,8) — это уязвимость в плагине Drag and Drop File Upload for Elementor Forms для WordPress до версии 1.6.0 включительно, которая позволяет атакующему без аутентификации загружать исполняемые файлы и выполнять код на сервере. Проблема связана с использованием контролируемого пользователем параметра `type` при проверке допустимых типов файлов и некорректной обработкой расширений.

CVE-2026-75865 (9,8) — это уязвимость в плагине WPLP Cookie Consent для WordPress до версии 4.4.1 включительно, которая позволяет атакующему без аутентификации загружать произвольные файлы с возможностью последующего выполнения кода. Проблема связана с

отсутствием проверки типа файла в функции загрузки логотипа и обходом авторизации в REST API коннектора WPLP.

CVE-2026-32475 (9,0) — это уязвимость в плагине Elementor Pro для WordPress до версии 4.2.1 включительно, которая позволяет атакующему без аутентификации загрузить PHP-файл через публичную форму и выполнить код на сервере. Проблема связана с различиями в обработке пустых файлов между этапами проверки расширений и сохранения загрузок в модуле Forms.

CVE-2026-14894 (9,8) — это уязвимость в плагине Super Forms — Drag & Drop Form Builder для WordPress до версии 6.3.313 включительно, которая позволяет атакующему без аутентификации загружать исполняемые файлы и выполнять код на сервере. Проблема связана с отсутствием проверки типов файлов и прав доступа в обработчике отправки формы; используемый защитный nonce доступен неавторизованным посетителям.

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

Данный топ включает в себя уязвимости в популярных сервисах: Keycloak, WordPress, Langflow. Две уязвимости WordPress являются частями цепочки описанных выше атак.

CVE	Описание	Количество
CVE-2026-63030	Это критическая уязвимость путаницы маршрутов (route confusion) в конечной точке пакетного обработчика REST API в ядре WordPress	90
CVE-2026-33017	В Langflow версиях до 1.9.0 конечная точка POST /api/v1/build_public_tmp/{flow_id}/flow позволяла создавать публичные потоки без аутентификации.	27
CVE-2026-64638	Это уязвимость отраженного межсайтового скриптинга (XSS) на странице входа WordPress	26
CVE-2026-87902	Это критическая уязвимость обхода каталога (path traversal) и локального включения файлов (LFI) в ядре WordPress, позволяющая неавторизованному злоумышленнику выполнять произвольный код (RCE) при определенных условиях.	26
CVE-2026-18963	Это критическая уязвимость (оценка CVSS 9.1 из 10) в компоненте keycloak-services платформы Keycloak и Red Hat Build of Keycloak (RHBK), связанная с нарушением проверки состояния в процессе сброса пароля	15

Отдельно про XSS

В этом отчете мы упомянули о сразу двух RCE-уязвимостях в WordPress. Хотя они опасны сами по себе, первичным триггером была XSS-уязвимость.

XSS позволяет злоумышленнику выполнить JavaScript-код в браузере пользователя в контексте уязвимого сайта. В статьях о последствиях XSS чаще всего упоминают кражу данных, фишинг и перенаправление на рекламные или вредоносные ресурсы. Однако последствия не ограничиваются браузером: в сочетании с возможностями приложения или дополнительными уязвимостями XSS может привести к компрометации сервера.

Рассмотрим веб-интерфейс роутера или панель управления сервером. В некоторых таких системах администратору доступны функции выполнения команд (интерактивные shell), редактирования файлов или установки расширений. Если злоумышленнику удастся выполнить свой JavaScript-код в контексте этого интерфейса в браузере авторизованного администратора, он потенциально сможет воспользоваться этими функциями от его имени.

Например, пользователь с ограниченными правами может внедрить вредоносный код в поле, содержимое которого впоследствии отображается администратору без безопасной обработки. При открытии такой страницы сработает хранимая XSS. Другой возможный сценарий связан с отраженной XSS: администратор переходит по специально подготовленной ссылке, и код выполняется в его браузере.

Кража пароля или сессионных данных при этом необязательна. Вредоносный скрипт может отправлять запросы к приложению, используя активную сессию администратора. Если доступные функции и права позволяют, это может привести к выполнению команд на сервере или размещению веб-шелла, то есть серверного скрипта для удаленного управления.

Атака может остаться незаметной для администратора. Его сеанс продолжает работать, логин и пароль не меняются, а уведомление о новом входе может не появиться, поскольку действия выполняются через уже авторизованный браузер.

Пример подобной цепочки описан в CVE-2024-46538. Пользователь с правом редактирования групп интерфейсов мог внедрить хранимую XSS. Когда администратор открывал соответствующую страницу, внедренный код использовал доступную ему функцию выполнения команд. Другие примеры, описанные нами выше, Click2Shell и т. д.

Кроме того, внедренный через XSS JavaScript-код может эксплуатировать уязвимости самого браузера, например его движка V8. Пользователь открывает привычный сайт, а вредоносный скрипт запускает эксплойт, который при наличии подходящей уязвимости позволяет выполнить произвольный машинный код в процессе браузера. В сочетании с уязвимостью, позволяющей выйти из браузерной песочницы, такая атака может привести к компрометации компьютера пользователя.

Заключение

Самый яркий тренд, который виден в результатах нашего анализа, — лавинообразный рост уязвимостей в годовом выражении (почти в 4 раза), главной причиной которого, скорее всего, является то, что нейросети (AI-инструменты) стали полноценным рабочим инструментом для автоматического анализа кода и быстрого создания инструментов для взлома. И мы, и другие эксперты в индустрии предсказывали это событие, и, кажется, именно в третьем квартале оно стало реальностью.

Растет и количество уязвимостей в самих AI-сервисах. Технологии искусственного интеллекта не только помогают атаковать, но и сами становятся мишенью. Доля уязвимостей в AI-платформах (таких как Langflow, MLflow, LiteLLM) выросла с 4,8 до 7,3%, а средняя критичность этих дыр аномально высока — **8,83 балла**. Вывод: IT-рынок внедряет AI быстрее, чем успевает его защищать. Как мы уже отмечали раньше, это довольно стандартный подход: рынок AI очень конкурентный, и разработчики стремятся выпустить продукт быстрее других, но от этого страдает безопасность, и это угроза, прежде всего, для пользователей таких сервисов.

Еще один важный вывод: сетевой вектор имеют 87,9% всех уязвимостей, и подавляющее большинство из них эксплуатируется через самый массовый протокол — HTTP (84,9%). Защита веб-ресурсов (сайтов, порталов, облачных API) — это теперь 90% всей видимой безопасности компании.

Появление более сложных уязвимостей в WordPress. Если раньше основной проблемой WordPress были сотни уязвимых плагинов, то в третьем квартале вдобавок к ним появились громкие цепочки уязвимостей (**Wp2shell, Click2Shell**), бьющие напрямую в ядро самой платформы.

Заметным стал рост угроз для экосистемы Apache. Продукты компании Apache (особенно интеграционный фреймворк Apache Camel) показали колоссальный скачок по числу найденных уязвимостей — рост с 12 до 69 за один квартал. Это дает понимание, насколько быстро может появляться информация, доказывающая уязвимость продукта. Современным AI-агентам достаточно краткой информации об уязвимости, а также двух версий продукта (уязвимой и исправленной), чтобы весьма точно определить, что именно было исправлено и как могла эксплуатироваться исправленная уязвимость. В будущем это может привести к появлению большого количества приватных 1-day-эксплойтов. Особенно этот риск актуален для продуктов, распространяемых по свободной модели.

Эксплойты стали критически доступны: 97,4% сообщений об уязвимостях содержат Proof-of-Concept. Время между моментом, когда ИБ-исследователи находят дыру, и моментом, когда ее начинают массово использовать хакеры, сокращается.

Как защититься

1. **Реагировать быстро**
   Так как 97,4% уязвимостей имеют готовые инструкции для взлома в открытом доступе, скорость реакции ИБ-команд становится ключевым параметром для безопасности IT-инфраструктуры организации. С обновлением браузеров сотрудников, CMS, инфраструктурного ПО и сетевого оборудования не стоит медлить, так как атакующие уже имеют инструменты для автоматизированной массовой эксплуатации вновь открытых уязвимостей практически сразу после публикации PoC.
2. **Следить за AI-сервисами**
   AI — новая зона риска в инфраструктуре организаций. Если ваши разработчики или аналитики используют инструменты вроде Langflow, MLflow или LiteLLM, их необходимо взять под строгий ИБ-контроль. В частности, стоит изолировать среды разработки, ограничивать права контейнеров, используемых для работы AI-моделей.
3. **Обучайте сотрудников**
   Цепочки уязвимостей вроде *Click2Shell* работают только в том случае, если администратор сайта перейдет по фишинговой ссылке злоумышленника. Обучите ИТ-администраторов и контент-менеджеров никогда не кликать по подозрительным ссылкам.
4. **Разделите права пользователей**
   Ограничивайте права сотрудников внутри корпоративных систем (CMS, CRM, GitLab). Ошибки десериализации данных или обхода каталогов (CWE-22, CWE-94) часто позволяют пользователю с низкими правами захватить права администратора, если система настроена некорректно.

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.

Wp2shell

CVE-2026-41452

Click2Shell