# Выпущен nginx 1.31.9

18 ноября 2026 года вышел nginx 1.31.9. Обновление mainline-ветки устраняет десять уязвимостей. В выпуск также вошли изменения обработки запросов и исправления ошибок.

## Исправления безопасности

- В некоторых конфигурациях с директивами `try_files` и `alias` в рабочем процессе могло произойти переполнение буфера (**CVE-2026-125283**).
- Переполнение окна управления потоком HTTP/2 позволяло вызвать segmentation fault в рабочем процессе и потенциально могло иметь другие последствия (**CVE-2026-123007**).
- При недостаточном значении `worker_connections` использование HTTP/2 могло приводить к обращению к освобождённой памяти (use-after-free) (**CVE-2026-123633**).
- Аналогичная ошибка use-after-free при недостаточном `worker_connections` устранена для HTTP/3 (**CVE-2026-121810**).
- При использовании `resolver` и одновременном разрешении одного имени в подзапросах могла возникнуть ошибка use-after-free. Злоумышленник, способный инициировать разрешение имени, мог вызвать segmentation fault и потенциально другие последствия (**CVE-2026-123634**).
- В почтовом прокси устранена ошибка use-after-free в рабочем процессе (**CVE-2026-113425**).
- В модуле Stream при синхронном завершении SSL-рукопожатия клиентский сертификат мог проверяться по настройкам сервера по умолчанию вместо виртуального сервера, выбранного по SNI (**CVE-2026-120967**).
- Модуль `ngx_stream_ssl_preread_module` мог интерпретировать некорректные сообщения ClientHello иначе, чем другие реализации TLS, что могло приводить к обходу ограничений безопасности (**CVE-2026-123640**).
- При чтении тела запроса через SSL рабочий процесс мог попадать в бесконечный цикл (**CVE-2026-118899**).
- При использовании PROXY protocol версии 2 с динамической загрузкой SSL-сертификатов в рабочем процессе мог произойти segmentation fault (**CVE-2026-120993**).

## Изменения обработки запросов

- Строки заголовков без двоеточия теперь отклоняются.
- Запрос отклоняется, если тело с передачей chunked содержит чрезмерный объём служебных данных разметки.

## Исправления ошибок

- Устранено переполнение буфера при использовании базы GeoIP в формате MMDB с некорректными координатами.
- Исправлено зависание запроса при проксировании во время отбрасывания его тела.
- Исправлено декодирование некоторых значений статической таблицы QPACK в HTTP/3.
- В HTTP/2 трейлеры ответа больше не задерживают данные потоков с более высоким приоритетом.
- Переменные `$cookie_...` и модуль `ngx_http_userid_module` теперь корректно обрабатывают заголовок `Cookie`, содержащий cookie без имени.
- Исправлено вычисление некэшируемых переменных в директиве `index`.
- Исправлено кэширование OCSP-ответов для клиентских сертификатов с нестандартными серийными номерами при использовании `ssl_ocsp_cache`.
- Control API теперь отвечает на запросы со слишком длинной строкой запроса.

Источник: список изменений nginx.