# Выпущен OpenVPN 2.7.8

Выпущен OpenVPN 2.7.8. Это корректирующий релиз, в котором устранены несколько проблем безопасности, ужесточена проверка сертификатов и исправлены ошибки в механизме DCO.

## Исправления безопасности

- В полях subject сертификата теперь проверяется наличие нулевых байтов. Сертификаты с такими полями отклоняются как недействительные. Исправление закрывает уязвимость **CVE-2026-84790**, о которой сообщил Вивек Парих.
- При TLS-рукопожатии с `tls-crypt-v2` клиент больше не пытается добавить обёрнутый клиентский ключ, если ключевой материал отсутствует. Ошибка проявлялась при некорректном поведении сервера. CVE ей не присвоен: по критериям CRA возможность вредоносного сервера нарушить работу клиента не считается отдельной уязвимостью.
- При очистке `domain_search_list` устранено переполнение беззнакового целого типа — **CVE-2026-88964**. Ошибку обнаружил и исправил Коул Мунц.
- В Windows командный интерпретатор `cmd.exe` больше не выполняет подстановку переменных внутри аргументов, заключённых в кавычки. Исправление закрывает **CVE-2026-84256**, о которой сообщил Даррен Каррерас.

## Изменения, заметные пользователям

- Проверка сертификатов стала строже относиться к нулевым байтам в строках. Это может нарушить работу существующих конфигураций с такими сертификатами при использовании сборок с OpenSSL. Сборки с mbedTLS отклоняли их и раньше.
- При наличии в сертификате повторяющихся полей, например нескольких CN, сборки с OpenSSL использовали последнее значение, а сборки с mbedTLS — первое. Поведение mbedTLS изменено и теперь совпадает с OpenSSL.

## Исправления ошибок

- DCO теперь удаляет установленные `iroute` при отключении клиента, а не во время отложенной очистки экземпляра. Это устраняет состояние гонки при переподключении клиентов, из-за которого в системе могли отсутствовать все `iroute`. Об ошибке сообщила команда OpenVPN Inc Access Server.
- В DCO для Linux устранены оставшиеся состояния гонки между синхронными операциями netlink и входящими асинхронными уведомлениями. Для этого добавлен второй netlink-сокет, а синхронные и асинхронные операции строго разделены.
- Клиент отклоняет переданную сервером комбинацию формата данных epoch с шифрами, не относящимися к AEAD. Вместо завершения работы с фатальной

ошибкой клиент перезапускает сессию.
- При ошибке создания нового узла или установки для него ключевого материала DCO в Linux и Windows больше не завершает весь процесс OpenVPN. Ошибка передаётся выше по стеку вызовов, после чего перезапускается соответствующий экземпляр. TLS-рукопожатие подвержено состоянию гонки: ядро может удалить узел из-за ошибки транспорта или тайм-аута, пока пользовательское пространство ещё не знает об этом и пытается, например, установить новые ключи. Такая ошибка критична для конкретного клиентского экземпляра, но не должна останавливать весь сервер.
- DCO больше не запрашивает статистику узла при отключении клиента. Прежний код должен был обеспечивать точность счётчиков, но к моменту запроса узел уже удалялся из ядра, поэтому OpenVPN получал только сообщение об ошибке. Кроме того, реализация была неэффективной, поскольку каждый раз опрашивала все узлы. Корректная передача итоговых счётчиков сессии будет реализована отдельно с помощью данных из уведомления ядра `DEL_PEER`.
- На сервере p2mp улучшена обработка списков `mbuf` при широковещательном и многоадресном трафике. Также исправлена ошибка при отключении клиента, которая в редких случаях могла приводить к взаимной блокировке очереди сервера.

Подробности доступны в официальном описании выпуска и полном списке изменений между OpenVPN 2.7.7 и 2.7.8.