НКЦКИ
НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru
E-mail: threats@cert.gov.ru



# Эксплуатация критических уязвимостей в NGINX (CVE-2026-113425, CVE-2026-121810, CVE-2026-123007, CVE-2026-123633, CVE-2026-123634)

ALRT-20261119.2 | 19 ноября 2026 г.

Уровень угрозы: КРИТИЧЕСКИЙ

TLP: WHITE

По каналам Национального координационного центра по компьютерным инцидентам получены сведения о пяти критических уязвимостях в программном обеспечении NGINX Open Source и NGINX Plus, получивших общее название NGINX2ROOT. Уязвимости позволяют неаутентифицированному злоумышленнику удалённо выполнить произвольный код с привилегиями рабочего процесса NGINX, либо вызвать ошибку типа «отказ в обслуживании».

Уязвимости затрагивают механизмы обработки HTTP/2 и HTTP/3, взаимодействия с upstream-серверами, динамического разрешения DNS-имен в директиве proxy_pass, а также работу почтового прокси-сервера с механизмом auth_http. Эксплуатация возможна только при наличии соответствующей конфигурации. Наиболее высокому риску подвержены общедоступные серверы с включенным HTTP/2 или HTTP/3.

Официальные исправления выпущены 18 ноября 2026 г. в версиях NGINX Open Source 1.30.7 и 1.31.9, а также NGINX Plus 37.0.8.1 и 37.3.0.1.

Детализация уязвимостей:

Описание угрозы

CVE-2026-113425, ошибка использования данных после освобождения памяти (Use-After-Free) в почтовом прокси-сервере и auth_http.

Уязвимость связана с ошибкой управления памятью в механизме аутентификации почтового прокси-сервера NGINX. При использовании директив proxy on и auth_http специально сформированная последовательность сетевых событий при обработке подключения может привести к обращению к уже освобожденной области памяти.

Для эксплуатации не требуется наличие действительных учетных данных пользователя. Уязвимость затрагивает конфигурации NGINX, используемые в качестве почтового прокси-сервера для IMAP, POP3 и SMTP с включенным механизмом auth_http.

Уязвимость затрагивает версии NGINX, начиная с 0.5.15.

CVE-2026-121810, ошибка использования данных после освобождения памяти (Use-After-Free) при обработке HTTP/3 и upstream.

Уязвимость связана с использованием освобожденной области памяти при обработке HTTP/3-соединений на базе QUIC и последующем перенаправлении запросов на upstream-серверы.

Эксплуатация может привести к аварийному завершению рабочего процесса NGINX, нарушению доступности сервиса или выполнению произвольного кода при определенных условиях.

Уязвимость затрагивает конфигурации с использованием HTTP/3 и проксированием запросов на upstream-серверы. Уязвимость затрагивает версии NGINX, начиная с 1.25.0.

CVE-2026-123007, переполнение при обработке HTTP/2 WINDOW_UPDATE.

Уязвимость связана с ошибкой управления окном передачи данных HTTP/2. Некорректное изменение значения окна при обработке управляющих кадров WINDOW_UPDATE может привести к переполнению целочисленного значения и последующему выполнению некорректной операции копирования данных в памяти.

Уязвимость затрагивает официальные версии NGINX, начиная с 1.9.5, при включенной поддержке и использовании HTTP/2.

CVE-2026-123633, ошибка использования данных после освобождения памяти (Use-After-Free) при обработке HTTP/2 и проксировании upstream.

Уязвимость связана с использованием освобожденной области памяти при обработке HTTP/2-соединений и перенаправлении запросов на upstream-серверы. При недостаточном количестве свободных соединений worker-процесса специально сформированный запрос может привести к повреждению памяти.

Уязвимость затрагивает конфигурации NGINX с поддержкой HTTP/2 и проксированием запросов на серверы upstream. Уязвимость затрагивает версии NGINX, начиная с 1.19.7.

CVE-2026-123634, ошибка использования данных после освобождения памяти (Use-After-Free) в механизме resolver, proxy_pass и mirror.

Уязвимость связана с ошибкой управления памятью в механизме разрешения DNS-имен (resolver). При использовании переменных в директиве proxy_pass, динамического разрешения имени upstream-сервера и механизма mirror с параметром mirror_request_body off специально сформированный HTTP-запрос может привести к использованию освобожденной области памяти.

Аналогичный уязвимый сценарий может возникать при использовании других механизмов создания дополнительных запросов, включая Server Side Includes (SSI).

Уязвимость затрагивает версии NGINX, начиная с 1.13.4 при наличии соответствующих условий конфигурации.

| | |
|---|---|
| Рекомендуемые меры по нейтрализации угроз | 1. Провести инвентаризацию инфраструктуры и проверить конфигурацию серверов с NGINX Open Source и NGINX Plus.<br>Особое внимание уделить наличию и использованию следующих функций:<br>– HTTP/2 и HTTP/3 (QUIC);<br>– proxy_pass, fastcgi_pass, grpc_pass и проксированию на upstream-серверы;<br>– директивам resolver и proxy_pass с переменными;<br>– механизмам mirror и SSI;<br>– почтовому прокси-серверу с директивами proxy on и auth_http.<br><br>2. Установить официальные обновления NGINX. Исправленные версии:<br>– NGINX Open Source: 1.30.7 (stable) и 1.31.9 (mainline);<br>– NGINX Plus: 37.0.8.1 и 37.3.0.1 -для CVE-2026-123007;<br>– NGINX Plus: 37.0.7.1 и 37.2.0.1 -для CVE-2026-123633;<br>– NGINX Plus: 37.0.8.1 и 37.3.0.1 -для CVE-2026-123634.<br>Для остальных уязвимостей необходимо проверить применимость исправлений к используемой линейке версий NGINX Plus по официальной информации F5/NGINX.<br><br>3. Проверить инфраструктуру на наличие признаков компрометации и настроить мониторинг попыток эксплуатации уязвимости. Убедиться, что на средствах защиты загружены актуальные сигнатуры. |