Простота эксплуатации CVE-2023-44487 делает её приоритетной целью для киберпреступников.

В августе 2023 года была выявлена критическая уязвимость в протоколе HTTP/2, известная как CVE-2023-44487 или Rapid Reset. Эта уязвимость, способная вызывать атаки типа "отказ в обслуживании" (DoS), стала серьёзной проблемой для интернет-сервисов и привлекла внимание киберпреступников. Компания Qrator Labs – это российская компания, специализирующаяся на обеспечении безопасности и стабильности сетей. Она предоставляет решения для защиты от DDoS-атак, мониторинга сетей и управления трафиком. Компания разрабатывает инновационные технологии и предоставляет услуги, которые помогают организациям защищать свои онлайн-ресурсы и обеспечивать надежную работу сетей. Qrator Labs является одним из лидеров в области кибербезопасности и сетевых решений в России и за её пределами, имея офисы в Чехии и Объединённых Арабских Эмиратах." data-html="true" data-original-title="Qrator Labs" >Qrator Labs поделилась информацией о функционировании CVE-2023-44487, её влиянии на HTTP/2 и предложила стратегии защиты.

HTTP/2 внедрил множество улучшений по сравнению с предыдущей версией протокола, включая мультиплексирование потоков, что позволяет открывать несколько потоков через одно TCP-соединение. Однако уязвимость Rapid Reset использует механизм отмены потока, применяя RST_STREAM кадры для нарушения работы сервера.

Когда пользователь заходит на веб-сайт, поддерживающий HTTP/2, одно соединение используется для нескольких ресурсов, что повышает эффективность взаимодействия. Однако такая возможность открывает двери для эксплуатации уязвимостей, поскольку одно соединение может генерировать множество запросов, увеличивая нагрузку на сервер. Для смягчения этой проблемы в HTTP/2 предусмотрен механизм ограничения количества активных одновременных потоков, предотвращающий перегрузку сервера клиентами.

Эксплуатация Rapid Reset заключается в отправке злоумышленником RST_STREAM кадра сразу после отправки запроса. Это заставляет сервер начать обработку запроса, но быстро отменяет его. Хотя запрос отменен, соединение HTTP/2 остаётся активным, что позволяет злоумышленнику повторять атаку, создавая новые потоки. В результате сервер тратит ресурсы на обработку отменённых запросов, что может привести к отказу в обслуживании.

Уязвимость Rapid Reset стала причиной масштабных распределённых атак типа DDoS.

Крупные компании, такие как Google, AWS и Cloudflare, сообщили о волнах атак, достигающих сотен миллионов запросов в секунду. Эти атаки проводились с использованием относительно небольших ботнетов, что подчеркивает серьёзность уязвимости.

Киберпреступники активно эксплуатируют уязвимость Rapid Reset, используя ее для проведения DDoS-атак. Простота эксплуатации и потенциальный ущерб сделали эту уязвимость главной мишенью для киберпреступников.

Компания Qrator Labs рекомендует применять следующие стратегии для защиты от уязвимости Rapid Reset:

Отслеживание подключений: Внимательно следить за статистикой подключений, включая количество активных потоков, скорость их создания и частоту отмены. Выявлять неправомерные подключения HTTP/2 и оценивать полезность каждого на основе содержимого запроса и поведения клиента. Закрывать соединения, демонстрирующие подозрительные паттерны.

Ограничение скорости: Реализовать механизмы управления трафиком на уровне соединений и потоков. Выявлять и блокировать подозрительные паттерны, такие как большое количество быстро отменённых потоков или запросов с известных вредоносных IP-адресов. Использовать адаптивное регулирование или очередь запросов для динамического управления ограничениями скорости в зависимости от серьёзности атаки.

Рекомендации для Apache: Настроить директивы MaxRequestWorkers и MaxConnectionsPerChild на веб-серверах Apache в соответствии с ёмкостью сервера и ожидаемым трафиком. Обновить libnghttp2 модуля mod_http2 до версии 1.57.0 или выше, включающей исправления уязвимости. Использовать дополнительные модули безопасности, такие как mod_security или mod_evasive, для усиления защиты.

Рекомендации для Nginx: Убедиться, что keepalive-ограничение по умолчанию не увеличено, чтобы не сделать сервер более уязвимым. При использовании нестандартных конфигураций с высокими ограничениями keepalive, перестроить Nginx из последней кодовой базы с патчем для предотвращения чрезмерного потребления ресурсов. Настроить директиву http2_max_concurrent_streams для ограничения количества одновременных потоков в зависимости от ёмкости сервера и ожидаемого трафика.

Qrator Labs также отметила, что уязвимость не затрагивает пользователей HAProxy благодаря защитным мерам, реализованным в версии 1.9 и перенесённым в последующие версии. Эти меры улучшают обработку мультиплексирования потоков протокола HTTP/2, что помогает противостоять атакам, подобным Rapid Reset. Вместо подсчёта только известных, установленных потоков, HAProxy 1.9 и более поздние версии учитывают выделенные ресурсы до их полного освобождения.