УЯЗВИМОСТЬ HTTP/2 RAPID RESET

Лифанов К.В., Рощупкин Н.А.

Белорусский государственный университет информатики и радиоэлектроники,

Минск, Республика Беларусь

Научный руководитель: Белоусова Е.С.– кандидат технических наук, доцент кафедры ЗИ

Аннотация. В материалах доклада представлены результаты исследования уязвимости протокола HTTP/2 (CVE-2023-44487), изучены и реализованы механизмы реализации DoS- и DDos-кибератак, в частности Rapid Reset Attack, на виртуальном макете, состоящем из веб-сервера и устройства нарушителя. Предложены методы ликвидации уязвимости веб-сервера, поддерживающим соединения по протоколу HTTP/2.

Ключевые слова: HTTP/2, CVE-2023-44487, DDoS, Nginx, Rapid Reset Attack

Введение

HTTP/2 – протокол, разработанный рабочей группой Hypertext Transfer Protocol working group. В мае 2015 года спецификация HTTP/2 была опубликована как RFC 7540. HTTP/2 был создан для решения проблемы увеличения временной задержки при передаче данных по протоколу HTTP/1. По статистике на данный момент протоколом HTTP/2 пользуются более 50% всех веб-ресурсов. Основными составляющими HTTP/2 стали фреймы (Frames) и потоки (Streams). В HTTP/2 есть функция мультиплексирования: все потоки посылаются в едином TCP соединении. Также в HTTP/2 есть специальный тип фреймов RST_STREAM, позволяющий прерывать определенный поток. Перечисленные функции HTTP/2 позволяет открыть несколько одновременных потоков в одном TCP соединении. Отмена потока реализуется посредством отправки RST_STREAM. Преимуществом такого соединения является то, что от клиента и сервера не требуется согласования отмены, она возможна в одностороннем порядке. Несмотря на преимущества новых функций протокола HTTP/2, у них есть уязвимости, одна из них CVE-2023-44487. Данная уязвимость является актуальной, так как для ее реализации не требуются значительные ресурсы.

CVE-2023-44487 – это уязвимость функции отправки фрейма RST_STREAM и функции мультиплексирования потоков протокола HTTP/2, которая может быть эксплуатирована путем открытия клиентом большого количества потоков одновременно, что приводит к ожиданию ответа от сервера на каждый поток запроса, при этом клиент немедленно отменяет каждый запрос. Таким образом, могут быть совершены DoS или DDoS кибератаки, в том числе Rapid Reset Attack, представленные на рисунке 1.

Основная часть

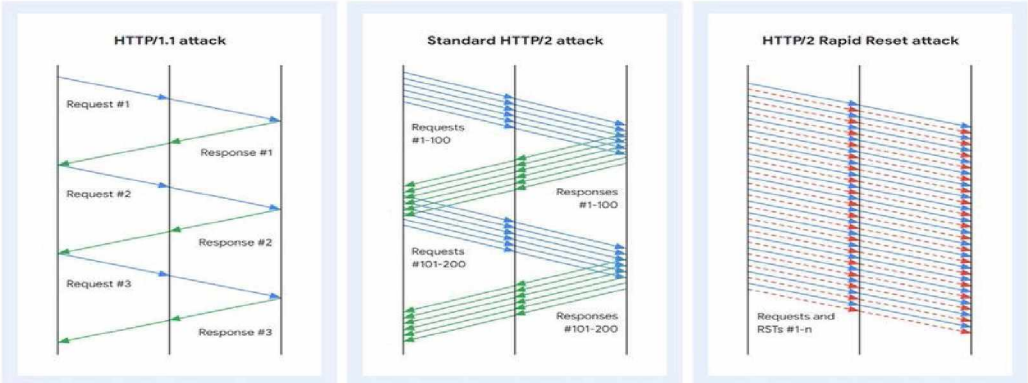
Для исследования уязвимости протокола HTTP/2 был создан макет, который включал в себя следующие виртуальные машины:

1 Веб-сервер на основе оперативной системе GNU/Linux Ubuntu Server 22.04 (ОЗУ 2 Гбайта, 1 vCPU).

2 Устройство потенциального нарушителя, с аналогичной ОС и равное по вычислительной мощности с сервером для корректности и наглядности сравнения.

Для работы веб-сервера было выбрано одно из самых распространенных ПО Nginx, за счет открытого исходного кода, удобству установки и конфигурации. Для использования протокола HTTP/2 необходима поддержка шифрования TLS посредством SSL-сертификатов, за счет чего осуществляется использование протокола HTTPS. Поэтому на веб-сервере были созданы самоподписанные SSL-сертификаты и произведена соответствующая конфигурация Nginx. Далее в конфигурационном файле веб-сервера в разделе «server» указывается строка «listen 443 ssl http2», которая включает поддержку HTTP/2.

Рисунок 1 – Механизмы реализации DoS и DDoS кибератак с использованием различных



версий протокола HTTP

Для реализации DoS кибератаки использовалась утилита, написанная на языке Go «rapidresetclient», позволяющая реализовать исследуемую кибератаку. Для контроля работы утилиты и просмотра отправляемых пакетов была использована программа «Wireshark», которая позволяет отследить количество, частоту и содержание HTTP-запросов.

Учитывая использование протокола HTTPS и его функции шифрования, для просмотра содержания пакетов было необходимо отредактировать исходный код «rapidresetclient» для

сохранения генерируемых ключей шифрования при установлении HTTPS-соединения и дальнейшего использования их для расшифровки пакетов. Как показано на рисунке 2, утилита исправно отправляет GET-запросы и запросы с флагом RST_STREAM поочередно, используя протокол HTTP/2, что и является реализацией Rapid Reset Attack.

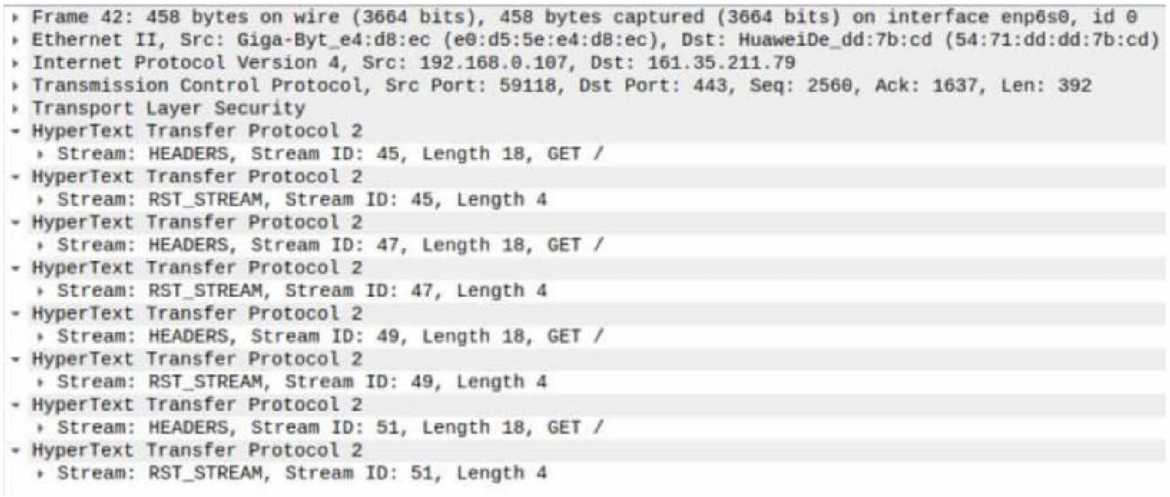


Рисунок 2 – Результат анализа пакетов с помощью Wireshark в ходе проведения Rapid Reset Attack

Для сравнения эффективности кибератак была произведена классическая DoS кибератака на протокол HTTP/1.1 с поддержкой HTTPS. Результаты сравнения двух кибератак представлены в таблице 1. В таблице 1 приводится значение «load average», которое отображает среднюю нагрузку системы, где «0» означает отсутствие нагрузки, «1» - отсутствие запаса производительности для 1-ядерного компьютера, а если значение больше, чем количество ядер процессора, значит система значительно перегружена и процессы ожидают своей очереди на исполнение.

Таблица 1 – Сравнение нагрузки при реализации Rapid Reset Attack и классической HTTP/1.1 кибератаке

Тип кибератаки	Кол-во запросов в секунду	Степень нагрузки процессора на сервере, %	Значение «load average» на сервере	Степень нагрузки процессора на устройстве нарушителя, %	Значение «load average» на устройстве нарушителя
HTTP/2 Rapid Reset Attack	8125	85–90	0,95–1,05	0,75–0,8	0,90
HTTP/1.1 DoS	234	84–86	0,60–0,65	86-90	44,5–48,0

Заключение

Результаты сравнения реализации Rapid Reset Attack и классической DoS кибератаке показали, что с точки зрения требований к вычислительной способности устройства нарушителя, кибератака на HTTP/2 намного эффективнее.

На основе изучения механизмов реализации DoS кибератак на веб-сервера, поддерживающие соединение по протоколу HTTP/2, были предложены способы ликвидации уязвимости CVE-2023-44487:

1 Ограничение количества открытых соединений и количества одновременно открытых потоков в рамках одного соединения.

2 Переход на HTTP/3.

3 Своевременное обновление серверного программного обеспечения.

Необходимо отметить, что первый способ не применим к сервисам, обрабатывающим большое количество пользователей одновременно. Также существуют коммерческие

решения от Cloudflare и других организаций, предоставляющих услуги в области кибербезопасности.

Список использованных источников:

1. *CVE-2023-44487 [Электронный ресурс]. – Режим доступа:* https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-44487. *– Дата доступа : 05.02.2024.*
2. *Создание самоподписанного SSL-сертификата для Nginx [Электронный ресурс]. – Режим доступа: https://www.8host.com/blog/sozdanie-samopodpisannogo-ssl-sertifikata-dlya-nginx-v-ubuntu-18-04/. – Дата доступа : 05.02.2024.*
3. *Tool for testing mitigations and exposure to Rapid Reset DDoS [Электронный ресурс]. – Режим доступа : https://github.com/secengjeff/rapidresetclient. – Дата доступа : 05.02.2024.*
4. *Best DDoS Attack Script Python3, Attack With 56 Methods [Электронный ресурс]. – Режим доступа : https://github.com/MatrixTM/MHDDoS. – Дата доступа : 05.02.2024.*