Amazon Web Services (AWS), Cloudflare y Google anunciaron el martes que tomaron medidas para contrarrestar ataques de denegación de servicio distribuidos (DDoS) sin precedentes que se basaron en una técnica innovadora llamada *«Reinicio Rápido de HTTP/2».*

Estos ataques de nivel 7 fueron detectados a finales de agosto de 2023, según lo informaron las compañías en una divulgación coordinada. La vulnerabilidad acumulativa a este tipo de ataque se encuentra registrada como CVE-2023-44487 y tiene una puntuación CVSS de 7.5 sobre un máximo de 10.

Mientras que los ataques dirigidos a la infraestructura en la nube de Google alcanzaron un punto máximo de 398 millones de solicitudes por segundo (RPS), aquellos dirigidos a AWS y Cloudflare superaron un volumen de 155 millones y 201 millones de solicitudes por segundo (RPS), respectivamente.

El Reinicio Rápido de HTTP/2 hace referencia a una vulnerabilidad de día cero en el protocolo HTTP/2 que puede ser explotada para llevar a cabo ataques DDoS. Una característica significativa de HTTP/2 es la capacidad de multiplexar solicitudes a través de una única conexión TCP, lo que se manifiesta en forma de flujos concurrentes.

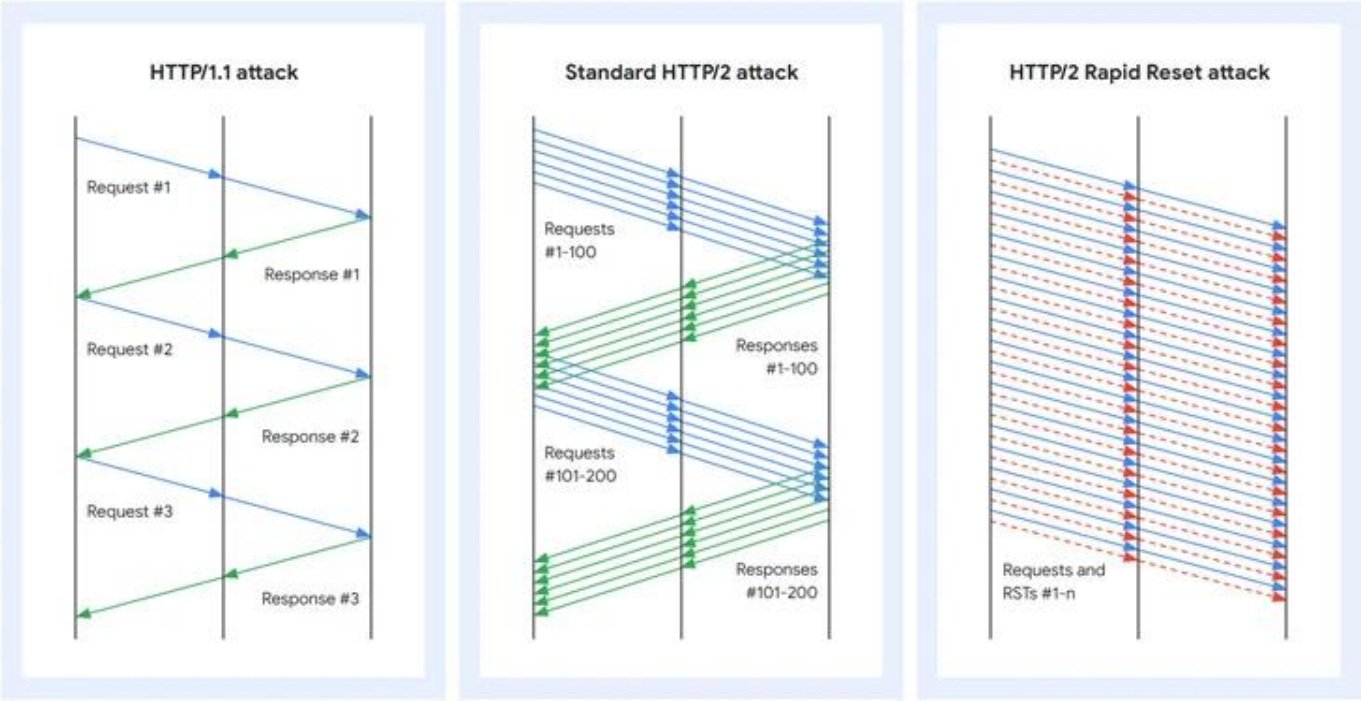
Además, un cliente que desee cancelar una solicitud puede emitir un marco RST_STREAM para detener el intercambio de datos. El ataque de «Reinicio Rápido» aprovecha este método para enviar y cancelar solicitudes en rápida sucesión, evitando así el límite de flujos concurrentes del servidor y sobrecargándolo sin llegar a su umbral de configuración.

> *«Los ataques de 'Reinicio Rápido de HTTP/2' constan de múltiples conexiones HTTP/2 con solicitudes y reinicios en rápida sucesión»,* señalaron Mark Ryland y Tom Scholl de AWS.

> *«Por ejemplo, se transmitirán una serie de solicitudes para múltiples flujos, seguidas de un reinicio para cada una de esas solicitudes. El sistema objetivo*

> *analizará y actuará sobre cada solicitud, generando registros para una solicitud que luego es reiniciada o cancelada por un cliente».*

Esta capacidad para reiniciar flujos de manera inmediata permite que cada conexión tenga un número indefinido de solicitudes en curso, lo que posibilita que un actor amenaza emita una oleada de solicitudes HTTP/2 que pueden sobrecargar la capacidad de un sitio web objetivo para responder a nuevas solicitudes entrantes, dejándolo inoperable en efecto.




En otras palabras, al crear cientos de miles de flujos HTTP/2 y anularlos rápidamente en gran cantidad a través de una conexión previamente establecida, los perpetradores de amenazas pueden abrumar sitios web y sacarlos de servicio. Un aspecto crucial adicional es que estos ataques pueden llevarse a cabo utilizando un botnet de tamaño moderado, alrededor de 20,000 máquinas, según lo observado por Cloudflare.

> *«Este día cero proporcionó a los atacantes una herramienta crítica y novedosa en su conjunto de vulnerabilidades, que les permite explotar y atacar a sus objetivos a una escala jamás vista antes»*, afirmó Grant Bourzikas, director de seguridad de Cloudflare.

Según W3Techs, el 35.6% de todos los sitios web utilizan HTTP/2. El porcentaje de solicitudes que usan HTTP/2 es del 77%, según datos compartidos por Web Almanac.

Google Cloud reportó que ha detectado varias versiones de los ataques de Reinicio Rápido que, aunque no son tan efectivas como la versión inicial, resultan más eficientes que los ataques DDoS estándar de HTTP/2.

> *«La primera variante no cancela de inmediato los flujos, sino que abre un lote de flujos a la vez, espera un tiempo y luego cancela esos flujos para luego abrir inmediatamente otro lote grande de flujos nuevos»,* explicaron Juho Snellman y Daniele Lamartino.

> *«La segunda variante elimina completamente la cancelación de flujos y, en su lugar, intenta abrir más flujos concurrentes de los que el servidor anunció de manera optimista».*

F5, en un aviso independiente, indicó que el ataque afecta al módulo NGINX HTTP/2 y ha recomendado a sus clientes actualizar la configuración de NGINX para limitar el número de flujos concurrentes a un máximo de 128 y mantener las conexiones HTTP durante hasta 1000 solicitudes.

> *«Después de hoy, es muy probable que los perpetradores de amenazas estén al tanto de la vulnerabilidad de HTTP/2; y sin duda se convertirá en algo sencillo de*

> *explotar, lo que marcará el comienzo de la carrera entre los defensores y los atacantes: quiénes aplicarán el parche primero contra quiénes serán los primeros en explotarla. Las organizaciones deben asumir que sus sistemas serán sometidos a pruebas y tomar medidas proactivas para garantizar la protección»,* agregó Bourzikas.