Centro Nacional de Seguridad Digital	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°241**	**Fecha: 11-10-2023**
		Página: 4 de 12

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Vulnerabilidad de día cero de reinicio rápido HTTP/2 explotada para lanzar ataques DDoS récord		
Tipo de Ataque	Denegación distribuida de servicio DDoS	Abreviatura	DDoS
Medios de propagación	Red, Correo, Navegación de Internet		
Código de familia	F	Código de Sub familia	F01
Clasificación temática familia	Disponibilidad del Servicio		

Descripción

1. ANTECEDENTES:

Amazon Web Services (AWS), Cloudflare y Google dijeron el martes que tomaron medidas para mitigar los ataques récord de denegación de servicio distribuido (DDoS) que se basaban en una técnica novedosa llamada HTTP/2 Rapid Reset.

Los ataques de capa 7 se detectaron a finales de agosto de 2023, dijeron las empresas en una divulgación coordinada. La susceptibilidad acumulada a este ataque se rastrea como **CVE-2023-44487** y tiene una puntuación CVSS de 7,5 sobre un máximo de 10.

2. DETALLES:

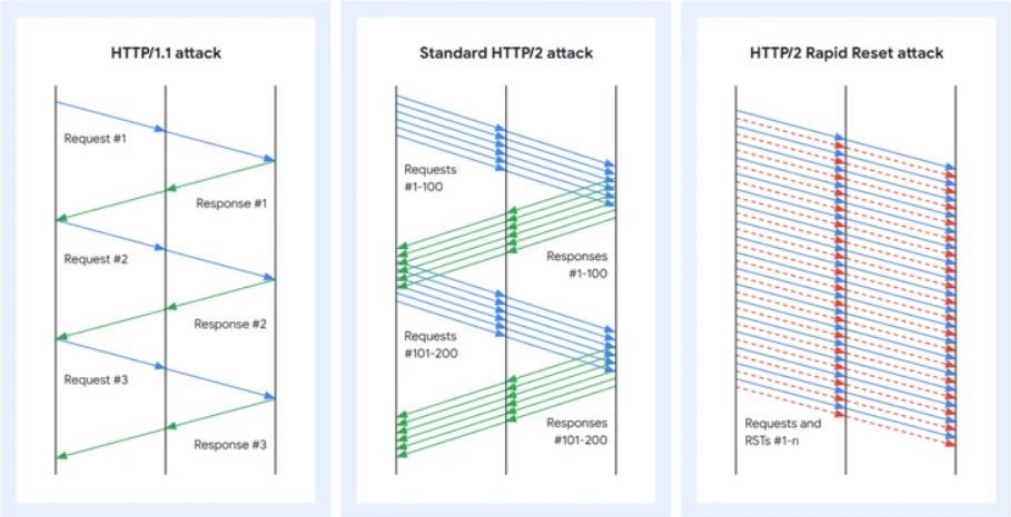
Mientras que los ataques dirigidos a la infraestructura de la nube de Google alcanzaron un máximo de 398 millones de solicitudes por segundo (RPS), los que afectaron a AWS y Cloudflare superaron un volumen de 155 millones y 201 millones de RPS, respectivamente. Esto vendría a ser 300% mayor que el mayor ataque DDOS de la historia.

HTTP/2 Rapid Reset se refiere a una falla de día cero en el protocolo HTTP/2 que puede explotarse para llevar a cabo ataques DDoS.

Una característica importante de HTTP/2 es la multiplexación de solicitudes a través de una única conexión TCP, que se manifiesta en forma de flujos simultáneos. El protocolo de red HTTP/2 dispone de un parámetro de servidor que autoriza un número definido de solicitudes al mismo tiempo. Las solicitudes que superen este número serán rechazadas.

Otra característica del protocolo HTTP/2 es la posibilidad de cancelar una solicitud. Es decir, un cliente que quiera cancelar una solicitud puede emitir una trama RST_STREAM para detener el intercambio de datos.

Esta técnica, que permite multiplexar de múltiples solicitudes en una sola conexión, se basa en automatizar la creación masiva de solicitudes de conexión y en su cancelación inmediata, creando un patrón de "solicitud, cancelación" a gran escala. El ataque Rapid Reset aprovecha este método para enviar y cancelar solicitudes en rápida sucesión, evitando así el flujo máximo concurrente del servidor y sobrecargando el servidor sin alcanzar su umbral configurado.



Por ejemplo, se transmitirá una serie de solicitudes para múltiples transmisiones 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 se restablecerá o cancelará mediante un cliente. Esta capacidad de restablecer transmisiones inmediatamente permite que cada conexión tenga una cantidad indefinida de solicitudes en curso.

Dicho de otra manera, al iniciar cientos de miles de transmisiones HTTP/2 y cancelarlas rápidamente a escala a través de una conexión establecida, los actores de amenazas pueden saturar los sitios web y dejarlos fuera de línea.

Lo que hace que este exploit sea aún más grave es que requiere una cantidad relativamente insignificante de recursos para lanzar un ataque. Los ataques DDOS a esta escala normalmente requieren cientos de miles o incluso millones de ordenadores infectados. El exploit HTTP/2 Rapid Reset sólo necesita 20.000 ordenadores infectados para lanzar ataques tres veces mayores que los mayores ataques DDOS jamás registrados.

Google Cloud dijo que ha observado múltiples variantes de los ataques Rapid Reset que, si bien no son tan efectivos como la versión inicial, son más eficientes que los ataques DDoS HTTP/2 estándar.

"La primera variante no cancela inmediatamente las transmisiones, sino que abre un lote de transmisiones a la vez, espera un tiempo, luego cancela esas transmisiones y luego abre inmediatamente otro gran lote de nuevas transmisiones", dijeron Juho Snellman y Daniele Lamartino.

"La segunda variante elimina por completo la cancelación de transmisiones y, en cambio, intenta con optimismo abrir más transmisiones simultáneas de las que anuncia el servidor".

Recursos Afectados:

- Cualquier empresa o usuario, aplicación web, servicio o API en un servidor o proxy capaz de comunicarse utilizando el protocolo HTTP/2 podrían ser vulnerables.
- Módulo NGINX HTTP/2 (ngx_http_v2_module).
- Apache Tomcat, versiones:
  - Desde 8.5.0 hasta 8.5.93.
  - Desde 9.0.0-M1 hasta 9.0.80.
  - Desde 10.1.0-M1 hasta10.1.13.
- Listado de productos afectados de Microsoft IIS.

3. RECOMENDACIONES:

- Actualizar la configuración del módulo NGINX HTTP/2 para limitar la cantidad de transmisiones simultáneas a un valor predeterminado de 128 y persistir las conexiones HTTP hasta 1000 peticiones.
- Actualizar Apache Tomcat a las versiones 8.5.94, 9.0.81 y 10.1.14.
- Desactivar el protocolo HTTP/2 en el servidor web mediante el Registry Editor.
- Eliminar la referencia a http2 en la parte de escucha del archivo de configuración del servidor web y aplicar las recomendaciones aportadas en el blog de Cloudfare.

Fuente de Información:	• hxxps://thehackernews.com/2023/10/http2-rapid-reset-zero-day.html?_m=3n%2e009a%2e3171%2emv0ao44squ%2e25sa • hxxps://www.incibe.es/incibe-cert/alerta-temprana/avisos/vulnerabilidad-0day-en-protocolo-http2-rapid-reset • hxxps://piratageglory.com/es/la-vulnerabilidad-ddos-http-2-rapid-reset-afecta-practicamente-a-todos-los-sitios/