Un equipo de investigadores chinos encontró una nueva forma de abusar de los paquetes HTTP para amplificar el tráfico web y reducir los sitios web y redes de entrega de contenido (CDN).

Denominada RangeAmp, esta técnica de denegación de servicio (DoS), explota implementaciones incorrectas del atributo HTTP *«Solicitudes de rango».*

Las solicitudes de rango HTTP son parte del estándar HTTP y permiten a los clientes (generalmente navegadores), solicitar solo una porción específica (rango) de un archivo de un servidor. La función se creó para pausar y reanudar el tráfico en situaciones controladas (acciones de pausa o reanudación) o no controladas (congestión o desconexiones de la red).

El estándar HTTP Range Requests ha estado en discusión en Internet Engineering Task Force (IETF) por más de media década, pero, debido a su utilidad, ya fue implementado por navegadores, servidores y CDN.

Ataques RangeAmp descubiertos

El equipo de investigadores afirma que los atacantes pueden usar solicitudes de rango HTTP malformadas para amplificar la forma en que los servidores web y sistemas CDN reaccionan cuando tienen que lidiar con una operación de solicitud de rango.

El equipo cree que existen dos ataques RangeAmp distintos. El primero se denomina RangeAmp Small Byte Range (SBR), en el que el atacante envía una solicitud de rango HTTP con formato incorrecto al proveedor de CDN, que amplifica el tráfico hacia el servidor de destino, y finalmente bloquea el sitio objetivo.

El segundo, RangeAmp Overlapping Byte Ranges (OBR), donde el atacante envía una solicitud de rango HTTP con formato incorrecto a un proveedor de CDN, y el tráfico se canaliza por medio de otros servidores CDN, el tráfico se amplifica dentro de las redes CDN y bloquea los servidores CDN haciendo que dichos servidores y muchos otros sitios de destino sean inaccesibles.

Según los investigadores, al probar los ataques RangeAmp contra 13 proveedores de CDN, descubrieron que todos eran vulnerables al ataque RangeAmp SBR, y seis también eran vulnerables a la variante OBR cuando se utilizaban en ciertas combinaciones.

Afirmaron que los ataques son muy peligrosos y requerían un mínimo de recursos para llevarse a cabo. De los dos, los ataques RangeAmp SBR podrían amplificar más el tráfico.

El equipo descubrió que los atacantes podrían usar un ataque RangeAmp SBR para inflar el tráfico de 724 a 43,330 veces el tráfico original.

Los ataques OBR RangeAmp fueron un poco más difíciles de llevar a cabo, debido a que las seis CDN vulnerables necesitaban estar en configuraciones específicas (maestro-sustituto), pero cuando se cumplieron las condiciones, los investigadores dijeron que los ataques OBR también podrían usarse para inflar el tráfico dentro de una red CDN con factores de amplificación de hasta casi 7500 veces el tamaño del paquete inicial.

De los dos, los ataques OBR se consideraron más peligrosos, ya que los atacantes podían eliminar fragmentos enteros de la red de un proveedor de CDN, lo que reducía la conectividad de miles de sitios web a la vez.

Los investigadores dijeron que durante los últimos siete meses, se han comunicado de forma silenciosa con los proveedores de CDN afectados y revelaron los detalles del ataque RangeAmp.

De los 13 proveedores de CDN, 12 respondieron de forma positiva e implementaron o dijeron que planeaban implementar actualizaciones para su implementación de Solicitud de Rango HTTP.

La lista incluye Akamai, Alibaba Cloud, Azure, Cloudflare, CloudFront, CDNsun, CDN77, Fastly, G-Core Labs, Huawei Cloud, KeyCDN y Tencent Cloud.

> *«Desafortunadamente, aunque les enviamos correos electrónicos varias veces y tratamos de comunicarnos con sus servicios al cliente, StackPath no proporcionó ningún comentario»,* dijo el equipo de investigación.
>
> *«En general, hemos hecho todo lo posible para informar de forma responsable las vulnerabilidades y proporcionar soluciones de mitigación. Los proveedores de CDN relacionados han tenido casi siete meses para implementar técnicas de mitigación antes de que se publicara este documento».*

La respuesta de cada proveedor de CDN, junto con los detalles técnicos acerca de los ataques RangeAmp, están disponibles en el documento del equipo de investigación, bajo el título *«CDN Backfired: Amplification Attacks Based on HTTP Range Requests»,* disponible aquí.

Este documento será presentado en julio en la conferencia virtual IEEE/IFIP DSN 2020, siendo uno de los tres nominados para el premio al mejor artículo.