Un grupo de investigadores alemanes seguridad cibernética, descubrió un nuevo ataque de envenenamiento de caché contra sistemas de almacenamiento en caché web, que podría ser utilizado por un hacker para obligar a un sitio web específico a entregar páginas de error a la mayoría de sus visitantes en lugar de contenido o recursos legítimos.

El problema afecta a los sistemas de caché de proxy inverso como Varnish y algunos servicios de Redes de Distribución de Contenido (CDN) ampliamente utilizados, incluidos Amazon CloudFront, Cloudflare, Fastly, Akamai y CDN77.

En resumen, una red de distribución de contenido (CDN), es un grupo de servidores distribuidos geográficamente que se encuentran entre el servidor de origen de un sitio web y sus visitantes para optimizar el rendimiento del sitio web.

Un servicio CDN almacena en caché, archivos estáticos, incluyendo páginas HTML, archivos JavaScript, hojas de estilo, imágenes y videos, desde el servidor de origen y los entrega a los visitantes más rápido sin tener que volver al servidor de origen una y otra vez.

Cada uno de los servidores CDN distribuidos geográficamente, conocidos como nodos perimetrales, también comparten la copia exacta de los archivos de caché y los sirve a los visitantes en función de su ubicación.

Por lo general, luego de un tiempo definido o cuando se purga manualmente, los servidores CDN actualizan el caché al recuperar una nueva copia actualizada de cada página web del servidor de origen y almacenaras para futuras solicitudes.

Apodado como CPDoS, abreviatura de Denegación de Servicio Envenenado en Caché, el ataque reside en la forma en que los servidores CDN intermedios están configurados incorrectamente para almacenar en caché los recursos web o páginas con respuestas de error devueltas por el servidor de origen.

El ataque CPDoS amenaza la disponibilidad de los recursos web de un sitio con solo enviar

una solicitud HTTP que contiene un encabezado con formato incorrecto, según tres académicos alemanes, Hoai Viet Nguyen, Luigi Lo Iacono y Hannes Federrath.

> *«El problema surge cuando un atacante puede generar una solicitud HTTP para un recurso almacenable en caché donde la solicitud contiene campos inexactos que son ignorados por el sistema de almacenamiento en caché, pero generan un error mientras es procesado por el servidor de origen».*

El modo de trabajo de CPDoS es el siguiente:

- Un atacante remoto solicita una página web de un sitio web de destino mediante el envío de una solicitud HTTP que contiene un encabezado con forma incorrecto.
- Si el servidor CDN intermedio no tiene una copia del recurso solicitado, reenviará la solicitud al servidor web de origen, que se bloqueará debido al encabezado mal formado.
- Como consecuencia, el servidor de origen devuelve una página de error, que finalmente es almacenada por el servidor de almacenamiento en caché en lugar del recurso solicitado.
- Ahora, cada vez que los visitantes legítimos intenten obtener el recurso de destino, recibirán la página de error en caché en lugar del contenido original.
- El servidor CDN también extenderá la misma página de error a otros nodos periféricos de la red de CDN, haciendo que los recursos específicos del sitio web de la víctima no estén disponibles.

> *«Cabe mencionar que una simple solicitud es suficiente para reemplazar el contenido original en la memoria caché por una página de error. Esto significa que dicha solicitud permanece por debajo del umbral de detección de firewalls de aplicaciones web (WAF) y medios de protección DDoS, en particular, mientras escanean grandes cantidades de tráfico de red irregular»,* dijeron los investigadores.

> *«Además, CPDoS puede explotarse para bloquear, por ejemplo, parches o actualizaciones de firmware distribuidas por medio de cachés, evitando la reparación de vulnerabilidades en dispositivos y software. Los atacantes también pueden desactivar importantes alertas de seguridad o mensajes en sitios web de misión crítica como banca en línea o sitios web gubernamentales».*

Para llevar a cabo estos ataques de envenenamiento de caché contra CDN, la solicitud HTTP con formato incorrecto puede ser de tres tipos:

HTTP Header Oversize (HHO): Una solicitud que contiene un encabezad de gran tamaño que funciona en escenarios en los que una aplicación web utiliza un caché que acepta un límite de tamaño de encabezado mayor que el servidor de origen.

HTTP Meta Character (HMC): En lugar de enviar un encabezado de gran tamaño, este ataque intenta omitir un caché con un encabezado de solicitud que contiene un metacarácter dañino, como salto de línea, retorno de carro, avance de línea o campana.

Anulación de método HTTP (HMO): Uso del encabezado de anulación HTTP para omitir la política de seguridad que prohíbe las solicitudes DELETE.

Los servicios de CDN son vulnerables a los ataques de CPDoS

Los investigadores llevaron a cabo tres ataques contra diferentes combinaciones de sistema de almacenamiento en caché web e implementaciones HTTP y descubrieron que CloudFront CDN de Amazon, es el más vulnerable al ataque CPDoS.

> *«Analizamos el comportamiento de almacenamiento en caché de páginas de error de quince soluciones de almacenamiento en caché web y las contrastamos con las especificaciones HTTP. Identificamos un producto de caché proxy y cinco servicios CDN que son vulnerables a CPDoS».*

El equipo de investigadores informó sus hallazgos a los proveedores de implementación HTTP y proveedores de caché afectados el pasado 19 de febrero de 2019. El equipo de Amazon Web Services (AWS) confirmó las vulnerabilidades en CloudFront y resolvió el problema prohibiendo el almacenamiento en caché de páginas de error con el código de estado 400, Solicitud Incorrecta por Defecto.

Microsoft también reconoció los problemas informados y publicó una actualización para mitigar esta vulnerabilidad, asignada como CVE-2019-0941, en sus actualizaciones de seguridad mensuales de junio de 2019.

Play Framework también confirmó los problemas informados y parchó su producto contra el ataque CPDoS al limitar el impacto del encabezado X-HTTP-Method-Override en las versiones 1.5.3 y 1.4.6 de Play Framework.

Otros proveedores afectados, como Flask, fueron contactados varias veces, pero los investigadores no obtuvieron respuesta.

Puedes obtener más detalles acerca de este ataque de envenenamiento de caché web y sus variantes, descargando el documento de investigación titulado *«Su caché ha caído: ataque de denegación de servicio envenenado por caché».*