¿Qué es el contrabando de solicitudes HTTP y la degradación de HTTP/2?

Entrevista de preguntas y respuestas con Love Andren, auditor junior de seguridad de aplicaciones, Ghostlabs AppSec en Outpost24

por The Gurus 1 de febrero de 2024 en Noticias, opiniones y análisis del editor

AT&T Cybersecurity aumenta la oferta de SASE al agregar Palo Alto Networks

Compartir en Facebook

Compartir en Twitter

¿Has oído hablar del término contrabando de solicitudes HTTP? ¿Qué pasa con la degradación de HTTP/2? Bueno, estas son vulnerabilidades que los ciberdelincuentes pueden aprovechar cuando hay problemas entre el front-end y el back-end de los sitios web. Si no se resuelven, estos problemas pueden tener consecuencias muy nefastas para cualquier empresa. El gurú de la seguridad de TI conversó con Love Andren, auditora junior de seguridad de aplicaciones de Ghostlabs AppSec en Outpost24, para comprender más sobre esta amenaza.

Gurú de la seguridad de TI (ISG): ¿Qué es el contrabando de solicitudes HTTP?

Love: un exploit que abusa del hecho de que el servidor web permite dos métodos separados al calcular la longitud del cuerpo, Transfer-Encoding y Content-Length. Si ambos se envían en una sola solicitud, podría provocar que el servidor de aplicaciones para el usuario o el servidor de servicios de fondo interpreten la solicitud de forma incorrecta, lo que provocaría una desincronización en el servidor de servicios de fondo. Cuando se hace correctamente, permitiría a un atacante pasar de contrabando una segunda solicitud HTTP dentro de la primera, y luego la respuesta se entregaría a la persona que emita la siguiente solicitud a la aplicación.

Las técnicas más comunes se basan en especificar la longitud del cuerpo de la solicitud en un valor menor que el cuerpo de la solicitud real. Esto luego hace que el servidor front-end o back-end crea que la solicitud finaliza en un punto determinado, y la parte restante del cuerpo que contiene la solicitud maliciosa se contrabandea.

El impacto abarca desde sesiones de secuestro, eludiendo el control de acceso hasta ataques de secuencias de comandos entre sitios.

ISG – ¿Qué es la degradación de HTTP/2?

Amor: si bien HTTP/2 se usa ampliamente, todavía hay servidores back-end heredados que usan exclusivamente HTTP/1, ya que aún es nuevo. Dado que una solicitud HTTP/2 comparada con HTTP/1 es similar en cuanto a estructura (no en la forma en que se envían), es un proceso sencillo convertir la solicitud a la sintaxis de los demás. Una diferencia principal e importante es que HTTP/2 no tiene que especificar la longitud de los cuerpos de la solicitud, ya que la solicitud/respuesta se envía como bytes.

Los problemas comienzan cuando el servidor front-end comienza a aceptar encabezados que no debería aceptar, especificando la longitud de la solicitud. Por ejemplo, enviar una solicitud HTTP/2 a la aplicación con un cuerpo que contiene otra solicitud, pero especificando la longitud del cuerpo en "0", podría hacer que el servidor de aplicaciones para el usuario las vea como dos solicitudes separadas al convertir a HTTP/1.1.

A su vez, esto reintroduce el contrabando de solicitudes en escenarios HTTP/2.

ISG – ¿Por qué las organizaciones/equipos de seguridad deben estar conscientes de estas amenazas? ¿A qué puede conducir?

Amor: la razón principal es el impacto de un ataque de contrabando de solicitudes exitoso, como se mencionó anteriormente. Todos los enumerados anteriormente tienen implicaciones catastróficas para una aplicación web.

Otra razón es la complejidad del exploit en sí; Es posible que se pase por alto al planificar o se omita para centrarse en exploits más comunes y fáciles de ejecutar (como XSS o problemas de autorización).

ISG – ¿Cree que esta amenaza se volverá más prominente en 2024 y más allá?

Amor – Es difícil para mí decirlo. Personalmente, creo que si los ingenieros de seguridad se familiarizan más con este complejo exploit, los posibles ataques podrían mitigarse. Lo mismo ocurre con los piratas informáticos éticos y los probadores de penetración: probar o ser mejores en las pruebas de ataques de contrabando podría generar clientes más felices.

ISG – ¿Cómo se puede mitigar el contrabando de solicitudes?

Amor: para el contrabando de solicitudes basado en HTTP/1, solo permita uno de los dos encabezados para determinar la longitud y asegúrese de que tanto el servidor front-end como el back-end estén configurados para usar el mismo. Bloquee solicitudes ambiguas y asegúrese de verificar siempre el cuerpo de la solicitud independientemente de lo que especifique la longitud.

Para el contrabando de solicitudes introducido por HTTP/2, asegúrese de que la comunicación HTTP/2 de extremo a extremo esté habilitada. Si se utiliza un servidor heredado y es necesario degradarlo, bloquee las solicitudes que contengan encabezados HTTP/1 especificando el tamaño del cuerpo. Otra mitigación es bloquear otras técnicas utilizadas en ataques de contrabando de solicitudes, como las inyecciones de secuencia CRLF.