Un grupo de investigadores detalló una nueva vulnerabilidad de tiempo en el protocolo Transport Later Security (TLS), que podría permitir a un atacante romper el cifrado y leer comunicaciones confidenciales en condiciones específicas.

Nombrado como Raccoon Attack, el ataque del lado del servidor explota un canal lateral en el protocolo criptográfico (versiones 1.2 y anteriores), para extraer la clave secreta compartida utilizada para las comunicacones seguras entre dos partes.

> *«La causa fundamental de este canal lateral es que el estándar TLS fomenta el procesamiento en tiempo no constante del secreto DH. Si el servidor reutiliza claves efímeras, este canal lateral puede permitir que un atacante recupere el secreto del premaster resolviendo una instancia del problema del número oculto»,* dijeron los investigadores.

Sin embargo, los investigadores aseguran que la vulnerabilidad es difícil de explotar y se basa en mediciones de tiempo muy precisas y en una configuración de servidor específica para ser explotada.

El uso de mediciones de tiempo para comprometer un criptosistema y filtrar información sensible ha sido el objetivo de muchos ataques de tiempo, y Raccoon emplea la misma estrategia para el proceso de intercambio de claves Diffie-Hellman (DH) durante un protocolo de enlace TLS, que es crucial para intercambiar datos en una red pública de forma segura.

Esta clave secreta compartida generada durante el intercambio permite una navegación segura en Internet, lo que permite a los usuarios visitar sitios web de forma segura al proteger las comunicaciones contra escuchas y ataques de intermediarios (MitM).

Para romper este muro de seguridad, la parte malintencionada registra los mensajes del protocolo de enlace entre un cliente y el servidor, utilizándolos para iniciar nuevos protocolos de enlace con el mismo servidor, y posteriormente, midiendo el tiempo que tarda el servidor en responder a las operaciones implicadas en la derivación de los datos compartidos.

Cabe señalar que *«los secretos DH con ceros a la izquierda darán como resultado un cálculo KDF del servidor más rápido, y por lo tanto, un tiempo de respuesta del servidor más corto».*

Suponiendo que el atacante puede identificar este caso extremo, le permite al atacante descifrar la clave secreta del protocolo de enlace original y, en última instancia, descifrar el tráfico TLS para recuperar su contenido en texto sin formato.

Sin embargo, el ataque tiene sus limitaciones. Requiere que el servidor reutilice la misma clave efímera DH (un modo llamado DHE) entre sesiones, y que el atacante esté lo más cerca posible del servidor de destino para realizar mediciones de tiempo de alta precisión.

F5, Microsoft, Mozilla y OpenSSL lanzan actualizaciones de seguridad

Aunque Raccoon puede ser difícil de replicar en el mundo real, se encontró que distintos productos F5 eran vulnerables a una versión *«especial»* del ataque (CVE-2020-5929), sin recurrir a mediciones de tiempo observando directamente el contenido de las respuestas del servidor.

F5, Microsoft, Mozilla y OpenSSL lanzaron parches para abordar la vulnerabilidad. Mozilla desactivó los conjuntos de cifrado DH y DHE en su navegador Firefox, y el aviso de Microsoft recomienda a los clientes que deshabiliten TLS_DHE.

> *«Nuestro ataque aprovecha el hecho de que los servidores pueden reutilizar el exponente DH secreto durante muchas sesiones, renunciando así al secreto»*, dijeron los investigadores.
>
> *«En este contexto, Raccoon enseña una lección para la seguridad de los protocolos:*

> *para los protocolos en los que una de las partes puede consultar continuamente algunos secretos criptográficos, la superficie de ataque se amplía. El ataque de Raccoon demostró que debemos tener cuidado al dar acceso a los atacantes a tales consultas»*, agregaron.