Investigadores de seguridad cibernética descubrieron un nuevo canal lateral que puede explotarse de manera confiable para filtrar información de los navegadores web que luego podría aprovecharse para rastrear a los usuarios incluso cuando JavaScript está completamente deshabilitado.

> *«Este es un ataque de canal lateral que no requiere JavaScript para ejecutarse. Esto significa que los bloqueadores de secuencias de comandos no pueden detenerlo. Los ataques funcionan incluso si elimina todas las partes divertidas de la experiencia de navegación web. Esto hace que sea muy difícil de prevenir sin modificar partes profundas del sistema operativo»,* dijeron los investigadores.

Al evitar JavaScript, los ataques de canal lateral también son arquitectónicamente agnósticos, lo que resulta en ataques de huellas dactilares de sitios web de microarquitectura que funcionan en plataformas de hardware, incluidas las CPU Intel Core, AMD Ryzen, Samsung Exynos 2100 y Apple M1, lo que lo convierte en el primer ataque de canal lateral conocido en conjuntos de chips basados en ARM de Apple.

Estos hallazgos provienen de un grupo de académicos de la Universidad Ben-Gurion del Negev, la Universidad de Michigan y la Universidad de Adelaide, y serán presentados en el Simposio de Seguridad de USENIX en agosto.

Los ataques de canal lateral generalmente se basan en datos indirectos como la sincronización, el sonido, el consumo de energía, las emisiones electromagnéticas, las vibraciones y el comportamiento de la caché en un esfuerzo por inferir datos secretos en un sistema. De forma específica, los canales laterales de microarquitectura explotan el uso compartido de los componentes de un procesador en el código que se ejecuta en diferentes dominios de protección para filtrar información secreta como claves criptográficas.

Además, los estudios también demostraron ataques totalmente automatizados como Rowhammer.js, que se basan únicamente en un sitio web con JavaScript malicioso para desencadenar fallas en el hardware remoto, obteniendo así acceso sin restricciones a los

sistemas de los visitantes del sitio web.

Aunque estos canales laterales con fugas se pueden tapar de forma efectiva mediante técnicas de aislamiento de dominio, los proveedores de navegadores han incorporado defensas para ofrecer protección contra ataques de tiempo y huellas dactilares al reducir la precisión de las funciones de medición del tiempo, además de agregar soporte para deshabilitar completamente JavaScript mediante complementos como NoScript.

Sin embargo, la última investigación publicada esta semana tiene como objetivo evitar esas mitigaciones basadas en el navegador mediante la implementación de un ataque de canal lateral llamado *«CSS Prime+Probe»*, construido únicamente con HTML y CSS, lo que permite que el ataque funcione aún en navegadores reforzados como Tor, Chrome, Zero y DeterFox, que tienen JavaScript completamente deshabilitado o limitan la resolución de la API del temporizador.

> *«Una tendencia común en estos enfoques es que son sintomáticos y no abordan la causa raíz de la fuga, es decir, el intercambio de recursos de microarquitectura. En cambio, la mayoría de los enfoques intentan evitar las fugas modificando el comportamiento del navegador, logrando distintos equilibrios entre seguridad y usabilidad»,* dijeron los investigadores.

Los canales laterales basados en caché se diferencian de los ataques Flush+Reload, en los que un espía puede usar una instrucción de borrado de caché para borrar líneas de caché específicas y determinar si la víctima accedió a estos datos.

Al volver a acceder a la misma línea de memoria y cronometrar el acceso para un acierto o fallar, Prime + Probe requiere que el atacante llene todo el caché compartido para desalojar los datos de la víctima, luego cronometra sus propios accesos después de que llena el caché.

La presencia de una falla en el caché indica que la víctima accedió a la línea de caché correspondiente, lo que provoca la eliminación de los datos del espía.

Aunque estos métodos explotan un canal de tiempo encubierto en el caché de la CPU, el nuevo ataque ideado por los investigadores de Ben-Gurion tiene como objetivo un canal lateral basado en caché en los navegadores web modernos.

Específicamente, la técnica CSS Prime+Probe se basa en renderizar una página web que incluye una variable de cadena HTML larga que cubre toda la caché, y luego realiza una búsqueda de una subcadena corta inexistente en el texto, lo que obliga a la búsqueda a escanear toda la cadena. En el paso final, el tiempo para llevar a cabo esta operación de sondeo se envía a un servidor controlado por el atacante.

> *«El atacante primero incluye en el CSS un elemento de un dominio controlado por el atacante, lo que fuerza la resolución del DNS. El servidor DNS malintencionado registra la hora de la solicitud de DNS entrante. Luego, el atacante diseña una página HTML que evoca una búsqueda de cadenas de CSS, probando efectivamente la caché. Esta búsqueda de cadenas va seguida de una solicitud de un elemento CSS que requiere resolución de DNS desde el servidor malicioso. Finalmente, la diferencia de tiempo entre las solicitudes de DNS consecutivas corresponde al tiempo que se tarda en realizar la búsqueda de cadenas, que es un proxy para la contención de caché»,* dijeron los investigadores.

Para evaluar la efectividad de los métodos a través de ataques de huellas dactilares en sitios web, los investigadores utilizaron el canal lateral mencionado antes, entre otros, para recopilar rastros del uso de caché mientras cargaban diferentes sitios web, incluidos los 100 sitios web principales de Alexa, utilizando los «memorygrams» para entrenar un modelo de red neuronal para identificar un conjunto específico de sitios web visitados por un objetivo.

Aunque los ataques de ocupación de caché basados en JavaScript ofrecen una mayor precisión de más del 90% en todas las plataformas en comparación con CSS Prime+Probe, el

estudio señaló que la precisión lograda por esta última es lo suficientemente alta como para filtrar datos que podrían permitir que las partes malintencionadas identifiquen y rastreen usuarios.

> *«Entonces, ¿cómo pueden los usuarios preocupados por la seguridad acceder a la web? Un factor que complica este concepto es el hecho de que el navegador web utiliza recursos compartidos adicionales más allá de la caché, como el sistema de resolución de DNS del sistema operativo, la GPU y la interfaz de red. La partición de la caché parece un enfoque prometedor, ya sea utilizando aislamiento basado en colores de caché, o por aislamiento temporal basado en SO»,* concluyeron los investigadores.