Un grupo de académicos ha desarrollado una innovadora forma de ataque de canal secundario denominada iLeakage, la cual explota una vulnerabilidad en las CPUs de las series A y M utilizadas en dispositivos de Apple con sistemas operativos iOS, iPadOS y macOS. Esto permite extraer información sensible del navegador web Safari.

> Según un nuevo estudio de los investigadores Jason Kim, Stephan van Schaik, Daniel Genkin y Yuval Yarom, *«un atacante puede inducir a Safari a representar una página web arbitraria y, posteriormente, recuperar información confidencial presente en ella mediante la ejecución especulativa».*

En un escenario de ataque práctico, esta debilidad podría ser aprovechada a través de una página web maliciosa para recuperar el contenido de la bandeja de entrada de Gmail e incluso obtener contraseñas almacenadas por los gestores de credenciales.

iLeakage, además de ser el primer caso de un ataque de ejecución especulativa al estilo de Spectre dirigido a las CPUs Apple Silicon, también afecta a todos los navegadores web de terceros disponibles para iOS y iPadOS debido a la política de la App Store de Apple, que requiere que los proveedores de navegadores utilicen el motor WebKit de Safari.

Apple fue informada de estos hallazgos el 12 de septiembre de 2022. Esta debilidad afecta a todos los dispositivos de Apple lanzados desde 2020 que funcionan con procesadores ARM de las series A y M de Apple.

La esencia del problema radica en que el código JavaScript malicioso y WebAssembly incrustado en una página web en una pestaña del navegador puede leer en secreto el contenido de un sitio web de destino cuando un usuario visita la página controlada por el atacante.

Esto se logra mediante un canal secundario microarquitectónico que puede ser utilizado por un actor malintencionado para inferir información sensible a través de otras variables como el tiempo, el consumo de energía o las emisiones electromagnéticas.

El canal secundario en el que se basa este último ataque es un mecanismo de optimización de rendimiento en las CPUs modernas conocido como ejecución especulativa, el cual ha sido objeto de varios métodos similares desde que Spectre salió a la luz en 2018.

Aunque la ejecución especulativa se concibió como un método para obtener ventajas en el rendimiento al aprovechar los ciclos de procesamiento disponibles para ejecutar instrucciones de programas fuera de secuencia cuando se encuentra una instrucción de bifurcación condicional cuya dirección depende de instrucciones previas cuya ejecución aún no ha concluido.

El fundamento de esta técnica consiste en predecir la ruta que seguirá el programa y ejecutar instrucciones de manera especulativa a lo largo de esa ruta. Cuando la predicción resulta ser acertada, la tarea se completa más rápidamente de lo que lo haría de otro modo.

Sin embargo, cuando se produce una predicción errónea, los resultados de la ejecución especulativa se descartan y el procesador retoma la ruta correcta. Dicho de otro modo, estas predicciones incorrectas dejan rastros en la memoria caché.

Ataques como Spectre implican inducir a una CPU a realizar operaciones especulativas que no se llevarían a cabo durante la ejecución correcta del programa y que revelan información confidencial de la víctima a través de un canal secundario.

En otras palabras, al forzar a las CPU a cometer errores en la predicción de instrucciones sensibles, la idea es permitir que un atacante (a través de un programa malicioso) acceda a los datos asociados con otro programa (es decir, la víctima), rompiendo efectivamente las protecciones de aislamiento.

iLeakage no solo elude las medidas de fortalecimiento incorporadas por Apple, sino que también implementa un método sin temporizador y que es compatible con diversas arquitecturas. Este método se aprovecha de las condiciones de competencia para distinguir entre accesos exitosos y fallidos a la caché cuando dos procesos, uno asociado con el

atacante y otro con el objetivo, se ejecutan en la misma CPU.

Este mecanismo sirve como base para un canal oculto que en última instancia logra una lectura fuera de límites en cualquier parte del espacio de direcciones del proceso de representación de Safari, lo que da lugar a una filtración de información.

Aunque es poco probable que esta vulnerabilidad se utilice en ataques prácticos en el mundo real debido a la experiencia técnica requerida para llevarlo a cabo, la investigación subraya las amenazas continuas que plantean las vulnerabilidades de hardware, incluso después de todos estos años.

La noticia sobre iLeakage llega meses después de que los investigadores de ciberseguridad revelaran detalles de tres ataques de canal secundario: Collide+Power (CVE-2023-20583), Downfall (CVE-2022-40982) e Inception (CVE-2023-20569), que podrían explotarse para filtrar datos sensibles de las CPU modernas.

También sigue al descubrimiento de RowPress, una variante del ataque RowHammer en chips DRAM y una mejora sobre BlackSmith que puede usarse para provocar cambios de bits en filas adyacentes, lo que lleva a la corrupción o el robo de datos.