Un equipo de investigadores ha identificado un nuevo tipo de ataque de filtración de datos que afecta a las arquitecturas más recientes de las CPU que admiten la ejecución especulativa.

Conocido como GhostRace (CVE-2024-2193), este ataque es una variante de la vulnerabilidad de la CPU relacionada con la ejecución transitoria, denominada Spectre v1 (CVE-2017-5753). Este enfoque combina la ejecución especulativa con las condiciones de carrera.

> *«Todos los métodos de sincronización comunes implementados mediante ramificaciones condicionales pueden ser eludidos a nivel microarquitectónico en los caminos especulativos mediante un ataque de predicción de bifurcación incorrecta, convirtiendo todas las áreas críticas libres de carreras desde el punto de vista arquitectónico en Condiciones de Carrera Especulativas (SRCs), lo que permite a los atacantes filtrar información del objetivo»*, señalaron los investigadores.

Los resultados provienen del Grupo de Investigación en Seguridad de Sistemas de IBM Research Europe y de VUSec, este último responsable de otro ataque de canal lateral llamado SLAM, dirigido a procesadores modernos en diciembre de 2023.

Spectre hace referencia a una clase de ataques de canal lateral que explotan la predicción de bifurcaciones y la ejecución especulativa en las CPU modernas para acceder a datos privilegiados en la memoria, eludiendo las protecciones de aislamiento entre aplicaciones.

Aunque la ejecución especulativa es una técnica de optimización de rendimiento utilizada en la mayoría de las CPU, los ataques de Spectre se aprovechan del hecho de que las predicciones incorrectas dejan rastros de accesos a memoria o cálculos en las cachés del procesador.

> *«Los ataques de Spectre inducen a una víctima a realizar operaciones de manera*

> *especulativa que no ocurrirían durante el procesamiento estrictamente secuencial y en orden de las instrucciones del programa, lo que permite filtrar información confidencial de la víctima a través de un canal oculto al atacante»*, explicaron los investigadores detrás del ataque Spectre en enero de 2018.

Lo que hace que GhostRace sea destacado es que permite a un atacante no autenticado extraer datos arbitrarios del procesador utilizando condiciones de carrera para acceder a los caminos de código especulativo ejecutable mediante lo que se conoce como un ataque de Uso Después de Liberar (Use-After-Free) Especulativo Concurrente (SCUAF).

Una condición de carrera es una situación indeseable que se produce cuando dos o más procesos intentan acceder al mismo recurso compartido sin una sincronización adecuada, lo que conduce a resultados inconsistentes y abre una ventana de oportunidad para que un atacante realice acciones maliciosas.

> *«En cuanto a características y estrategia de explotación, una vulnerabilidad de SRC es similar a una condición de carrera clásica»*, explicó el Centro de Coordinación CERT (CERT/CC) en un aviso.
>
> *«Sin embargo, difiere en que el atacante explota dicha condición de carrera en un camino ejecutado transitoriamente que proviene de una bifurcación mal predicha (similar a Spectre v1), apuntando a un fragmento de código o gadget con condiciones de carrera que finalmente revela información al atacante.»*

El resultado neto es que permite a un atacante con acceso a los recursos de la CPU acceder a datos sensibles arbitrarios en la memoria del host.

> Según VUSec, *«cualquier software, como un sistema operativo, hipervisor, etc., que*

> *utilice ramificaciones condicionales para implementar primitivas de sincronización sin incluir instrucciones de serialización en esa ruta, y que se ejecute en cualquier microarquitectura (por ejemplo, x86, ARM, RISC-V, etc.) que permita la ejecución especulativa de ramificaciones condicionales, es vulnerable a las SRCs».*

Tras una divulgación responsable, AMD afirmó que su orientación existente para Spectre *«sigue siendo efectiva para mitigar esta vulnerabilidad»*. Los responsables del desarrollo del hipervisor de código abierto Xen reconocieron que todas las versiones se ven afectadas, aunque señalaron que es poco probable que represente una amenaza de seguridad importante.

> *«Por precaución, el equipo de seguridad de Xen ha proporcionado parches de fortalecimiento, que incluyen la incorporación de un nuevo mecanismo LOCK_HARDEN en x86, similar al BRANCH_HARDEN existente»*, explicó Xen.
>
> *«LOCK_HARDEN está desactivado de manera predeterminada, debido a la incertidumbre sobre la existencia de una vulnerabilidad en Xen y las dudas sobre el impacto en el rendimiento. Sin embargo, esperamos que se realice más investigación en esta área y consideramos prudente tener una medida de mitigación en su lugar».*