Investigadores de la Vrije Universiteit Amsterdam han dado a conocer un reciente ataque de canal lateral denominado SLAM que podría ser aprovechado para filtrar información confidencial de la memoria del kernel en las CPU actuales y futuras de Intel, AMD y Arm.

Este ataque representa una explotación integral de Spectre basada en una novedosa característica presente en las CPU de Intel llamada Linear Address Masking (LAM), así como en sus equivalentes análogos de AMD (conocidos como Upper Address Ignore o UAI) y Arm (referidos como Top Byte Ignore o TBI).

> Los expertos de VUSec explican que «*SLAM se vale de gadgets no enmascarados para permitir que un proceso de espacio de usuario filtre datos arbitrarios del kernel en formato ASCII, destacando que podría ser utilizado para revelar la contraseña raíz en cuestión de minutos a partir de la memoria del kernel».*

A pesar de que LAM se presenta como una medida de seguridad, el estudio revela irónicamente que esta característica degrada la seguridad y aumenta de manera «*dramática*» la superficie de ataque de Spectre, dando lugar a un ataque de ejecución transitoria que explota la ejecución especulativa para extraer datos sensibles mediante un canal encubierto en la caché.

> *«Un ataque de ejecución transitoria aprovecha los efectos secundarios microarquitecturales de las instrucciones transitorias, permitiendo a un adversario malintencionado acceder a información que normalmente estaría prohibida por los mecanismos de control de acceso arquitectónicos»,* señala Intel en su documentación terminológica.

Caracterizado como el primer ataque de ejecución transitoria dirigido a futuras CPU, SLAM se beneficia de un nuevo canal encubierto basado en una traducción de dirección no canónica

que facilita la explotación práctica de gadgets Spectre genéricos para filtrar información valiosa. Este afecta a las siguientes CPU:

- CPU de AMD existentes vulnerables a CVE-2020-12965
- Futuras CPU de Intel que admitan LAM (tanto de paginación de 4 como de 5 niveles)
- Futuras CPU de AMD que admitan UAI y paginación de 5 niveles
- Futuras CPU de Arm que admitan TBI y paginación de 5 niveles

> *«Los sistemas Arm ya mitigaron Spectre v2 y BHB, y se considera responsabilidad del software protegerse contra Spectre v1. Las técnicas descritas solo amplían la superficie de ataque de vulnerabilidades existentes como Spectre v2 o BHB al aumentar la cantidad de gadgets explotables»,* señala Arm en un aviso.

AMD también ha señalado las mitigaciones actuales de Spectre v2 para abordar la explotación de SLAM. En cambio, Intel tiene la intención de proporcionar orientación de software antes del lanzamiento futuro de procesadores Intel que admitan LAM. Mientras tanto, los mantenedores de Linux han desarrollado parches para desactivar LAM de forma predeterminada.

Estos resultados emergen aproximadamente dos meses después de que VUSec presentara Quarantine, un enfoque exclusivamente basado en software para mitigar ataques de ejecución transitoria y lograr un aislamiento de dominio físico mediante la partición de la caché de último nivel (LLC), asignando a cada dominio de seguridad acceso exclusivo a una porción diferente del LLC con el objetivo de eliminar canales encubiertos en el LLC.

> *«El aislamiento del dominio físico de Quarantine aísla diferentes dominios de seguridad en núcleos separados para evitar que compartan recursos microarquitectónicos locales centrales. Además, deja de compartir la LLC, dividiéndola entre los dominios de seguridad»,* dijeron los investigadores