De forma errónea se dijo que la causa raíz de varios ataques de ejecución especulativa previamente revelados contra procesadores modernos, como Meltdown y Foreshadow, fueron atribuidos al *«efecto de búsqueda previa»*, lo que provocó que los proveedores de hardware liberaran mitigaciones y contramedidas incompletas.

Un grupo de académicos de la Universidad de Tecnología de Graz y el Centro Helmholtz de Seguridad de la Información de CISPA, finalmente revelaron la razón exacta detrás del por qué las direcciones del kernel se almacenan en caché en primer lugar, y también presentaron varios ataques nuevos para explotar el problema previamente no identificado, permitiendo a los atacantes rastrear datos confidenciales.

La nueva investigación explica que los ataques de microarquitectura fueron en realidad, causados por la desreferenciación especulativa de los registros de espacio de usuario en el kernel, lo que no solo afecta a las CPU Intel más recientes con las últimas mitigaciones de hardware, sino también a varios procesadores modernos de ARM, IBM y AMD, que anteriormente se creía que no resultaban afectados.

> *«Descubrimos que los efectos reportados en varios artículos académicos durante los últimos cuatro años no se entendieron correctamente, lo que llevó a suposiciones incorrectas sobre las contramedidas»*, dijeron los investigadores.
>
> *«Este efecto de captación previa en realidad no está relacionado con las instrucciones de captación previa de software o los efectos de captación previa de hardware debido a los accesos a la memoria y, en cambio, es causado por la desreferenciación especulativa de los registros de espacio de usuario en el kernel».*

Además de analizar la causa raíz real del efecto de búsqueda previa, algunos otros hallazgos clave de la investigación son:

- Descubrimiento de varios ataques nuevos que explotan la causa raíz subyacente,

incluido un ataque de traducción de direcciones en contextos más restringidos, filtración directa de valores de registros en escenarios específicos y un exploit de Foreshadow de extremo a extremo dirigido a datos que no son de nivel 1.
- Un nuevo ataque de canal encubierto entre núcleos que, en algunos casos, podría permitir a los atacantes observar el almacenamiento en caché de la dirección (o valor) almacenada en un registro sin depender de la memoria compartida.
- Los dispositivos de *«captación previa»* de Spectre pueden filtrar de forma directa datos reales, lo que no solo hace que el ataque ZombieLoad sea eficiente en las CPU de Intel para filtrar datos confidenciales de los búferes internos o la memoria, sino que también impacta en las CPU que no son de Intel.
- El problema de la desreferenciación especulativa, en ciertos ataques como Rowhammer, ataques de caché y DRAMA, podría permitir a los atacantes recuperar las direcciones físicas de las variables de JavaScript y exfiltrar información a través de la ejecución transitoria de forma remota a través de un navegador web.

Además, los investigadores también demostraron que la vulnerabilidad Foreshadow en la CPU Intel podría explotarse incluso cuando las mitigaciones recomendadas están habilitadas. Esto es posible debido al hecho de que el ataque se puede montar en datos que no residen en la caché L1 en versiones del kernel que contienen gadgets de *«captación previa».*

El software del sistema se basa en el mecanismo de traducción de direcciones de la CPU para implementar el aislamiento entre diferentes procesos. Cada proceso tiene su propio espacio de memoria virtual y no puede acceder a direcciones de memoria física arbitrarias fuera de él.

La traducción de direcciones actúa como una capa intermedia que mapea el espacio de direcciones virtuales, que es utilizado por un programa.

El espacio de direcciones virtuales también incluye un espacio de direcciones del kernel para albergar los subprocesos del kernel de Linux, lo que facilita que el hardware subyacente maneje instrucciones privilegiadas de suprocesos de usuario en modo kernel.

Los kernels del sistema operativo se pueden proteger contra ataques de canal lateral de captación previa a través de una técnica llamada aislamiento de tabla de páginas del kernel (KPTI o KAISER), que impone un aislamiento estricto del kernel y del espacio de usuario, de modo que el hardware no contiene ninguna información sobre las direcciones del kernel mientras se ejecuta en modo usuario. Los investigadores encontraron que no garantiza una protección total contra los ataques de traducción de direcciones, donde un atacante intenta verificar si dos direcciones virtuales diferentes se asignan a la misma dirección física.

Dicho de otra forma, el *«ataque de traducción de direcciones permite que las aplicaciones sin privilegios obtengan direcciones del kernel arbitrarias en la caché, y por lo tanto, resuelvan direcciones virtuales a físicas en sistemas Linux de 64 bits».*

Aunque la línea de pensamiento original era que dichos ataques estaban relacionados con instrucciones de captación previa, el nuevo hallazgo demuestra lo contrario, validando así que KAISER no es una contramedida adecuada contra los ataques de canal lateral de microarquitectura en el aislamiento del kernel.

En su lugar, explota un dispositivo Spectre-BTB-SA-IP (Branch Target Buffer, misma dirección, en el lugar), para provocar una fuga de información, lo que provoca una ejecución especulativa, y además lleva a cabo ataques de Meltdown y Foreshadow (L1 Terminal Fault) sin pasar por alto las mitigaciones L1TF.

Spectre-BTB-SA-IP es una variante de la vulnerabilidad de Spectre que aprovecha el búfer de destino de rama, un componente similar a la caché en la CPU que se utiliza para la predicción de ramas, para realizar ataques dentro del mismo espacio de direcciones y la misma ubicación de la rama.

> *«El mismo efecto de captación previa se puede utilizar para realizar Foreshadow. Si hay un secreto presente en la caché L3 y la dirección del mapa físico directo se desprotege en el kernel del hipervisor, los datos se pueden recuperar en el L1. Esto vuelve a habilitar Foreshadow incluso con las mitigaciones de Foreshadow*

> *habilitadas si las mitigaciones de Spectre-BTB no relacionadas están deshabilitadas»,* dijeron los investigadores.
>
> *«La consecuencia es que podemos montar un ataque Foreshadow en kernels más antiguos parcheados contra Foreshadow con todas las mitigaciones habilitadas y en un kernel completamente parcheado si solo se deshabilitan las mitigaciones de Spectre-v2».*

Para resaltar más el impacto de los ataques de canal lateral, los investigadores establecieron un canal encubierto basado en caché que exfiltraba datos de un proceso que se ejecutaba en una CPU Intel Core i7-6500U a otro proceso sigiloso, logrando una velocidad de transmisión de 10 bit/s para retransmitir un total de 128 bytes desde el proceso emisor al receptor.

Además, los investigadores revelaron que es posible filtrar el contenido del registro de un enclave SGX de CPU de Intel utilizando un registro que está desreferenciado especulativamente, llamado *«Trampa de desreferencia»,* usándolo para recuperar un valor de 32 bits almacenado en un registro de 64 bits dentro de 15 minutos.

Finalmente, algunos ataques ahora se pueden montar de forma remota utilizando JavaScript en un navegador web y *«llenar los registros de 64 bits con un valor controlado por el atacante en JavaScript mediante WebAssembly».*

Para mitigar estos ataques, se recomienda que las CPU actuales habiliten las mitigaciones de Spectre-BTB, incluida Reptoline (abreviatura de «return trampoline»).