Más de seis años después de descubrirse la vulnerabilidad Spectre que afecta a los procesadores modernos, una investigación reciente ha revelado que los procesadores más recientes de AMD e Intel aún son vulnerables a ataques de ejecución especulativa.

El ataque, presentado por los investigadores Johannes Wikner y Kaveh Razavi de ETH Zürich, busca eludir la Barrera del Predictor de Rama Indirecta (IBPB) en chips x86, una medida importante contra los ataques de ejecución especulativa.

La ejecución especulativa es una función de optimización de rendimiento en la cual los procesadores modernos ejecutan ciertas instrucciones fuera de orden al predecir la dirección que tomará el programa, acelerando el proceso si el valor predicho resulta ser correcto.

Si se produce una predicción errónea, las instrucciones, denominadas «transitorias,» se invalidan antes de que el procesador pueda continuar con el valor adecuado.

Aunque los resultados de estas instrucciones transitorias no afectan directamente el estado arquitectónico del programa, aún pueden cargar ciertos datos sensibles en la memoria caché del procesador mediante una predicción forzada, exponiéndolos a un atacante que normalmente no tendría acceso a esa información.

Intel describe el IBPB como un *«mecanismo de control de ramas indirectas que establece una barrera, impidiendo que el software que se ejecutó antes de la barrera controle los objetivos predichos de ramas indirectas ejecutadas después de la barrera en el mismo procesador lógico».*

Este mecanismo es una medida contra la Inyección de Objetivo de Rama (BTI), conocida como Spectre v2 (CVE-2017-5715), un ataque de ejecución transitoria de cruce de dominios que utiliza predictores de rama indirecta para provocar la ejecución especulativa de un *«gadget de divulgación».*

Un «gadget de divulgación» permite que un atacante acceda a información confidencial de una víctima que normalmente no sería visible, y transmitirla a través de un canal encubierto.

Los recientes hallazgos de ETH Zürich muestran que un error de microcódigo en microarquitecturas de Intel, como Golden Cove y Raptor Cove, podría permitir eludir el IBPB. Este ataque ha sido descrito como la primera *«filtración Spectre de extremo a extremo entre procesos.»*

> El fallo de microcódigo *«conserva predicciones de ramas que pueden ser utilizadas después de que el IBPB debería haberlas invalidado. Esta especulación posterior a la barrera permite a un atacante sortear las barreras de seguridad impuestas por los contextos de proceso y las máquinas virtuales»*, explicaron los investigadores.

La variante del IBPB en AMD, según el estudio, también puede ser evadida debido a cómo el kernel de Linux aplica IBPB, lo que permite un ataque denominado Post-Barrier Inception (PB-Inception), el cual permite a un atacante sin privilegios acceder a memoria privilegiada en los procesadores AMD Zen 1(+) y Zen 2.

Intel ha lanzado un parche de microcódigo para abordar este problema (CVE-2023-38575, puntuación CVSS: 5.5). AMD, por su parte, está rastreando la vulnerabilidad como CVE-2022-23824, de acuerdo con un aviso emitido en noviembre de 2022.

> *«Los usuarios de Intel deben asegurarse de que su microcódigo esté actualizado. Los usuarios de AMD deben instalar las actualizaciones del kernel»,* señalaron los investigadores.

Esta divulgación llega meses después de que los investigadores de ETH Zürich detallaran nuevas técnicas de ataque RowHammer, denominadas ZenHammer y SpyHammer. SpyHammer utiliza RowHammer para inferir la temperatura de la DRAM con alta precisión.

> *«RowHammer es extremadamente sensible a variaciones de temperatura, incluso si*

> *son muy pequeñas (como ±1 °C). La tasa de error en los bits inducida por RowHammer aumenta (o disminuye) consistentemente al subir la temperatura, y algunas celdas de DRAM vulnerables a RowHammer muestran errores de bits solo a una temperatura específica»*, destacó el estudio.

Aprovechando la relación entre RowHammer y la temperatura, un atacante podría determinar la utilización de un sistema y medir la temperatura ambiente. Este ataque también podría comprometer la privacidad al usar las mediciones de temperatura para conocer los hábitos de una persona en su hogar, como los momentos en que entra o sale de una habitación.

> *«SpyHammer es un ataque simple y eficaz que puede monitorear la temperatura de sistemas críticos sin modificaciones ni información previa sobre el sistema de la víctima»,* indicaron los investigadores.
>
> *«SpyHammer podría representar una amenaza para la seguridad y privacidad de los sistemas hasta que se adopte una defensa completamente segura contra RowHammer, lo cual es un desafío importante debido a que la vulnerabilidad de RowHammer continúa agravándose con el avance de la tecnología».*