Los procesadores modernos de Intel, incluidos Raptor Lake y Alder Lake, han sido descubiertos como vulnerables a un nuevo ataque de canal lateral que podría ser explotado para revelar información sensible de los procesadores.

El ataque, denominado Indirector por los investigadores de seguridad Luyi Li, Hosein Yavarzadeh y Dean Tullsen, aprovecha las deficiencias identificadas en el Predictor de Rama Indirecta (IBP) y el Búfer de Objetivo de Rama (BTB) para superar las defensas actuales y comprometer la seguridad de las CPU.

> *«El Predictor de Rama Indirecta (IBP) es un componente de hardware en los procesadores modernos que predice las direcciones objetivo de las ramas indirectas»*, explicaron los investigadores.
>
> *«Las ramas indirectas son instrucciones de flujo de control cuya dirección objetivo se calcula en tiempo de ejecución, lo que hace difícil predecirlas con precisión. El IBP utiliza una combinación de historial global y dirección de rama para predecir la dirección objetivo de las ramas indirectas.»*

La idea básica es identificar vulnerabilidades en el IBP para lanzar ataques precisos de Inyección de Objetivo de Rama (BTI), también conocidos como Spectre v2 (CVE-2017-5715), que apuntan al predictor de rama indirecta de un procesador para provocar la divulgación no autorizada de información a un atacante con acceso de usuario local a través de un canal lateral.

Esto se logra mediante una herramienta personalizada llamada iBranch Locator que se utiliza para localizar cualquier rama indirecta, seguida de la realización de inyecciones precisas de IBP y BTP para ejecutar especulativamente.

Intel, que fue informada de los hallazgos en febrero de 2024, ha notificado desde entonces a otros proveedores de hardware/software afectados sobre el problema.

Como mitigaciones, se recomienda utilizar la Barrera del Predictor de Rama Indirecta (IBPB) de manera más agresiva y reforzar el diseño de la Unidad de Predicción de Ramas (BPU) incorporando etiquetas más complejas, cifrado y aleatorización.

La investigación se presenta en un momento en que las CPU de Arm han sido encontradas susceptibles a su propio ataque de ejecución especulativa llamado TIKTAG que apunta a la Extensión de Etiquetado de Memoria (MTE) para filtrar datos con una tasa de éxito superior al 95% en menos de cuatro segundos.

El estudio *«identifica nuevos gadgets TikTag capaces de filtrar las etiquetas MTE desde direcciones de memoria arbitrarias a través de la ejecución especulativa»*, dijeron los investigadores Juhee Kim, Jinbum Park, Sihyeon Roh, Jaeyoung Chung, Youngjoo Lee, Taesoo Kim y Byoungyoung Lee.

> *«Con los gadgets TikTag, los atacantes pueden eludir la defensa probabilística del MTE, aumentando la tasa de éxito del ataque a casi el 100%.»*
>
> En respuesta a la divulgación, Arm dijo *«MTE puede proporcionar un conjunto limitado de defensas deterministas de primera línea, y un conjunto más amplio de defensas probabilísticas de primera línea, contra clases específicas de exploits.»*
>
> *«Sin embargo, las propiedades probabilísticas no están diseñadas para ser una solución completa contra un adversario interactivo que sea capaz de fuerza bruta, filtrar o crear etiquetas de dirección arbitrarias.»*