Investigadores de seguridad cibernética revelaron una nueva técnica que podría usarse para eludir las mitigaciones de hardware existentes en los procesadores modernos de Intel, AMD y ARM, y organizar ataques de ejecución especulativa como Spectre para filtrar información confidencial de la memoria del host.

Los ataques como Spectre están diseñados para romper el aislamiento entre distintas aplicaciones aprovechando una técnica de optimización llamada ejecución especulativa en implementaciones de hardware de CPU para engañar a los programas para que accedan a ubicaciones arbitrarias en la memoria y así filtrar sus secretos.

Aunque los fabricantes de chips incorporaron defensas de software y hardware, incluyendo Reptoline, así como salvaguardas como la especulación restringida de rama indirecta mejorada (eIBRIS) y ARM CSV2, el último método demostrado por los investigadores de VUSec tiene como objetivo sortear todas estas protecciones.

Llamada Inyección de historial de rama (BHI o Spectre-BHB), es una nueva variante de los ataques Spectre-V2 (rastreada como CVE-2017-5715) que pasa por alto tanto eIBRS como CSV2, y los investigadores lo describen como un *«exploit ordenado punto a punto»* que filtra la memoria del kernel arbitraria en las CPU Intel modernas.

> *«Las mitigaciones de hardware evitan que el atacante sin privilegios inyecte entradas predictoras para el kernel»,* dijeron los investigadores.

> *«Sin embargo, el predictor se basa en un historial global para seleccionar las entradas de destino para ejecutar especulativamente. Y el atacante puede envenenar este historial de la zona de usuario para obligar al kernel a predecir de forma errónea objetivos de kernel más interesantes (es decir, dispositivos) que filtran datos»,* agregó el Grupo de Seguridad de Sistemas y Redes de la Vrije Universiteit Amsterdam.

Dicho de otra forma, un fragmento de código malicioso puede usar el historial de sucursales compartido, que se almacena en el búfer de historial de sucursales de la CPU (BHB), para influir en las bifurcaciones mal pronosticadas dentro del contexto del hardware de la víctima, lo que da como resultado una ejecución especulativa que luego se puede utilizar para inferir información que debería ser inaccesible de otra manera.

Es probable que BHI afecte a todas las CPU Intel y Arm que se vieron afectadas anteriormente por Spectre-V2, lo que llevó a ambas empresas a lanzar actualizaciones de software para solucionar el problema. Los conjuntos de chips de AMD, sin embargo, no se ven afectados por la vulnerabilidad.

Intel también recomienda a los clientes que deshabiliten los filtros de paquetes Berkeley extendidos (eBPF) sin privilegios de Linux, habiliten tanto eIBRS como la prevención en modo supervisor (SMEP) y agreguen *«LFENCE a dispositivos identificados específicos que se encuentren explotables».*

> *«Las mitigaciones [Intel eIBRS y Arm CSV2] funcionan según lo previsto, pero la superficie de ataque residual es mucho más significativa de lo que supusieron originalmente los proveedores»,* dijeron los investigadores.

> *«Sin embargo, encontrar dispositivos explotables es más difícil que antes, ya que el atacante no puede inyectar directamente objetivos predictores por medio de los límites de privilegios. Es decir, el núcleo no saltará especulativamente a objetivos arbitrarios proporcionados por el atacante, sino que solo ejecutará especulativamente fragmentos de código válidos ya ejecutados en el pasado».*