Los investigadores han descubierto dos novedosos métodos de ataque dirigidos a CPUs Intel de alta capacidad que podrían ser aprovechados para llevar a cabo un ataque de recuperación de clave contra el algoritmo de Estándar Avanzado de Encriptación (AES).

Los enfoques han sido conjuntamente denominados Pathfinder por un grupo de académicos de la Universidad de California San Diego, la Universidad de Purdue, UNC Chapel Hill, el Instituto de Tecnología de Georgia y Google.

«Pathfinder permite a los atacantes leer y manipular elementos cruciales del predictor de ramificaciones, lo que facilita dos tipos principales de ataques: reconstrucción del historial de flujo de control del programa y ejecución de ataques Spectre de alta resolución», comentó Hosein Yavarzadeh, el autor principal del artículo.

> *«Esto implica extraer imágenes secretas de bibliotecas como libjpeg y recuperar claves de encriptación de AES a través de la extracción de valores intermedios».*

Spectre es el término asignado a una categoría de ataques de canal secundario que explotan la predicción de ramificaciones y la ejecución especulativa en CPUs modernas para leer datos privilegiados en la memoria de una forma que evade las protecciones de aislamiento entre aplicaciones.

El enfoque de ataque más reciente se dirige a una característica en el predictor de ramificaciones conocida como Registro de Historial de Rutas (PHR) – que mantiene un registro de las últimas ramificaciones tomadas — para inducir predicciones de ramificaciones erróneas y hacer que un programa víctima ejecute rutas de código no deseadas, exponiendo de manera inadvertida sus datos confidenciales.

Concretamente, introduce nuevas primitivas que hacen posible manipular PHR, así como las tablas de historial de predicción (PHTs) dentro del predictor de ramificaciones condicionales (CBR) para filtrar datos de ejecución históricos y, en última instancia, desencadenar un exploit al estilo de Spectre.

En una serie de demostraciones esbozadas en el estudio, se ha constatado que el método es efectivo para extraer la clave de encriptación AES secreta, así como para filtrar imágenes secretas durante el procesamiento por la ampliamente utilizada biblioteca de imágenes libjpeg.

Tras una divulgación responsable en noviembre de 2023, Intel, en un aviso publicado el mes pasado, indicó que Pathfinder se basa en ataques Spectre v1 y que las medidas de mitigación previamente implementadas para Spectre v1 y canales secundarios tradicionales contrarrestan los exploits mencionados. No hay indicios de que afecte a las CPUs de AMD.

> *«Este estudio demuestra que el PHR es susceptible a filtraciones, revela datos no accesibles a través de los PHTs (resultados ordenados de ramificaciones repetidas, orden global de todos los resultados de ramificación), expone un conjunto mucho más amplio de códigos de ramificación como posibles puntos de ataque, y no puede ser contrarrestado (eliminado, oscurecido) utilizando técnicas propuestas para los PHTs»,* afirmaron los investigadores.