Los procesadores AMD lanzados desde 2011 hasta 2019, tienen vulnerabilidades previamente no reveladas que los dejan vulnerables a dos nuevos ataques de canal lateral diferentes, según una investigación publicada recientemente.

Conocidos como Take A Way, los nuevos vectores de ataque potenciales aprovechan el predictor de forma de caché de datos L1 (L1D) en la microarquitectura Bulldozer de AMD para filtrar datos confidenciales de los procesadores y comprometer la seguridad al recuperar la clave secreta utilizada durante el cifrado.

La investigación fue publicada por un grupo de académicos del Instituto de Investigación de Sistemas Informáticos y Aleatorios de la Universidad de Tecnología e Investigación de Graz (IRISA), quienes revelaron de forma responsable las vulnerabilidades de AMD en agosto de 2019.

> *«Somos conscientes de un nuevo documento técnico que afirma posibles vulnerabilidades de seguridad en las CPU de AMD, mediante el cual un actor malintencionado podría manipular una función relacionada con la memoria caché para transmitir potencialmente datos de usuario de forma no intencionada»*, dijo AMD en un aviso.

> *«Los investigadores luego emparejan esta ruta de datos con software conocido y mitigado o vulnerabilidades de canal lateral de ejecución especulativa. AMD cree que estos no son nuevos ataques basados en la especulación».*

Aunque la notificación no muestra más detalles sobre la mitigación del ataque, Vedad Hadzic, uno de los investigadores importantes en el documento, dijo que la vulnerabilidad sigue abierta a la explotación activa.

Los problemas de Intel en sus CPU, como Meltdown, Spectre, ZombieLoad y la falla más reciente de firmware CSME no reparable, la investigación hace recordar que ninguna

arquitectura de procesador es completamente segura.

Al igual que el ataque Intel Spectre, los exploits denominados como Collide+Probe y Load+Reload, manipulan el predictor de caché L1D antes mencionado para acceder a los datos que de otra forma deberían estar seguros e inaccesibles.

> *«Con Collide+Probe, un atacante puede monitorear los accesos a la memoria de la víctima sin conocer las direcciones físicas o la memoria compartida cuando comparte el tiempo un núcleo lógico. Con Load+Reload, explotamos la forma del predictor para obtener rastros de víctimas de acceso a la memoria de alta precisión en el mismo núcleo físico»*, dijeron los investigadores.

El predictor de modo de caché L1D es un mecanismo de optimización que tiene como objetivo reducir el consumo de energía asociado con el acceso a los datos en caché en la memoria.

> *«El predictor calcula un µTag utilizando una función hash indocumentada en la dirección virtual. Este µTag se utiliza para buscar la forma de caché L1D en una tabla de predicción. Por lo tanto, la CPU tiene que comparar la etiqueta de caché de una sola forma en lugar de todas las posibles maneras, reduciendo el consumo de energía».*

Los ataques de caché recientemente descubiertos funcionan mediante ingeniería inversa de esta función de hash para rastrear los accesos a la memoria desde un caché L1D. Mientras Collide+Probe explotan las colisiones µTag en el predictor de caché L1D de AMD, Load+Reload aprovecha la forma en que el predictor maneja las direcciones con alias en la memoria.

Ambas técnicas de ataque pueden emplearse para extraer datos sensibles de otro proceso,

compartiendo la misma memoria que el atacante o un proceso ejecuta en un núcleo lógico diferente de la CPU.

Para demostrar el impacto de los ataques de canal lateral, los investigadores establecieron un canal encubierto basado en caché que extrajo datos de un proceso que se ejecuta en la CPU AMD a otro proceso sigiloso, logrando una velocidad de transmisión máxima de 588.9 kB/s utilizando 80 canales en paralelo en el procesador AMD Ryzen Threadripper 1920X.

Debido a que los procesadores EPYC de AMD están siendo adoptados por plataformas populares en la nube como Amazon, Google y Microsoft, el hecho de que estos ataques puedan llevarse a cabo en un entorno en la nube es demasiado preocupante.

Además, los investigadores de seguridad pudieron organizar con éxito un ataque Collide+Probe en algunos navegadores comunes, como Chrome y Firefox, evitando la aleatorización del diseño del espacio de direcciones (ASLR) en los navegadores, reduciendo así la entropía y recuperando la información de dirección.

ASLR es una implementación de seguridad que se utiliza para aleatorizar y enmascarar las ubicaciones exactas del código y las áreas de datos clave dentro de la memoria de la CPU. Dicho de otra forma, impide que un atacante potencial adivine las direcciones de destino y salte a secciones específicas en la memoria.

> *«En Firefox, podemos reducir la entropía en 15 bits con una tasa de éxito del 98% y un tiempo de ejecución promedio de 2.33 s (σ = 0.03s, n = 1000). Con Chrome, podemos reducir correctamente los bits con una tasa de éxito del 86.1% y un tiempo de ejecución promedio de 2.90 s (σ = 0.25s, n = 1000)»*, agregaron los investigadores.

Mitigación del ataque

Una buena noticia es que los ataques pueden mitigarse por medio de una variedad de cambios en hardware, hardware y software o solo software, incluido el diseño del procesador de una manera que pueda permitir la deshabilitación dinámica del predictor de forma temporal y borrar el estado del modo predictor cuando se cambia entre el modo kernel y el modo usuario.

Esta no es la primera vez que se descubre que los procesadores AMD son vulnerables a los ataques de la CPU, incluido Spectre, lo que obliga a la compañía a lanzar una serie de parches.