Los investigadores de seguridad descubrieron otra vulnerabilidad que afecta a numerosos microprocesadores AMD e Intel más antiguos, que podrían eludir las defensas actuales y dar lugar a ataques de ejecución especulativa basados en Spectre.

Nombrado como Retbleed por los investigadores de ETH Zurich, Johannes Wikner y Kaveh Razavi, el problema se rastrea como CVE-2022-29900 (AMD) y CVE-2022-29901 (Intel), y los fabricantes de chips lanzan mitigaciones de software como parte de un proceso de divulgación coordinado.

Retbleed también es la última incorporación a una clase de ataques de Spectre conocidos como Spectre-BTI (CVE-2017-5715 o Spectre-V2), que explotan los defectos secundarios de una técnica de optimización llamada ejecución especulativa por medio de un canal lateral de sincronización para engañar a un programa para acceder a ubicaciones arbitrarias en su espacio de memoria y filtrar información privada.

La ejecución especulativa intenta llenar la canalización de instrucciones de un programa al predecir qué instrucción se ejecutará a continuación para obtener un aumento de rendimiento, mientras que también deshace los resultados de la ejecución si la suposición resulta ser incorrecta.

Los ataques como Spectre se aprovechan del hecho de que estas instrucciones ejecutadas erróneamente, como resultado de la predicción errónea, están destinadas a dejar rastros de la ejecución en el caché, lo que da como resultado un escenario en el que un programa no autorizado pueden engañar al procesador para que ejecute rutas de código incorrectas e inferir datos secretos pertenecientes a la víctima.

Dicho de otro modo, Spectre es una instancia de ataque de ejecución transitoria, que se basa en fallas de diseño de hardware para «influir» en qué secuencias de instrucciones se ejecutan especulativamente y filtrar claves de cifrado o contraseñas desde el espacio de direcciones de memoria de la víctima.

Esto, a su vez, se logra por medio de canales secundarios de microarquitectura como Flush+Reload que mide el tiempo necesario para realizar lecturas de memoria del caché que se comparte con la víctima, pero no antes de vaciar parte de la memoria compartida, lo que resulta en lecturas rápidas o lentas dependiendo de si la víctima accedió a la línea de caché monitoreada desde que fue desalojada.

Aunque se han diseñado medidas de seguridad como Reptoline (también conocido como *«trampolín de retorno»*) para evitar la inyección de destino de rama (BTI), Retbleed está diseñado para sortear esta contramedida y lograr la ejecución de código especulativo.

> *«Los reptolines funcionan reemplazando los saltos indirectos [ramas donde el objetivo de la rama se determina en el tiempo de ejecución] y las llamadas con retornos»,* dijeron los investigadores.

> *«Retbleed tiene como objetivo secuestrar una instrucción de retorno en el kernel para obtener la ejecución de código especulativo arbitrario en el contexto del kernel. Con suficiente control sobre los registros y/o la memoria en la instrucción de retorno de la víctima, el atacante puede filtrar datos arbitrarios del kernel».*

La idea central, en pocas palabras, es tratar las instrucciones de retorno como un vector de ataque para la ejecución de especulaciones y obligar a que las declaraciones se predigan como ramas indirectas, deshaciendo efectivamente las protecciones ofrecidas por Reptoline.

Como nueva línea de defensa, AMD introdujo lo que se conoce como Jmp2Ret, mientras que Intel recomendó utilizar la especulación restringida de rama indirecta mejorada (eIBRS) para abordar la vulnerabilidad potencial, incluso si se implementan mitigaciones de Reptoline.

«El sistema operativo Windows usa IBRS de forma predeterminada, por lo que no se requiere actualización», dijo Intel, señalando también que trabajó con la comunidad de Linux para hacer disponibles actualizaciones de software para la deficiencia.