Investigadores académicos revelaron detalles sobre la nueva clase de vulnerabilidades de canal lateral de ejecución especulativa en los procesadores Intel que afecta a todos los chips modernos, incluidos los chips utilizados en dispositivos Apple.

Después del descubrimiento de las vulnerabilidades del procesador Spectre y Meltdown a inicios del año pasado, que pusieron en riesgo a casi todas las computadoras del mundo, surgieron una y otra vez diferentes variaciones de dichas vulnerabilidades.

Ahora, un equipo de investigadores de seguridad de distintas universidades y empresas, descubrió vulnerabilidades de canal lateral de ejecución especulativa diferentes pero más peligrosas en las CPU de Intel.

Estas fallas podrían permitir a los hackers robar de forma directa a nivel de usuario, así como secretos a nivel de sistema de los buffers de la CPU, incluidas las claves de usuario, contraseñas y claves de cifrado del disco.

Le ejecución especulativa es un componente central del diseño de los procesadores modernos que ejecuta instrucciones de forma especulativa basándose en suposiciones que se consideran probables. Si las suposiciones resultan válidas, la ejecución continúa, de lo contrario se descartan.

La muestra más nueva de vulnerabilidades de la microarquitectura (ataques MDS) consiste en cuatro fallas diferentes que, a diferencia de los ataques existentes que filtran datos almacenados en cachés de la CPU, pueden filtrar datos en vuelo arbitrarios de búferes internos de la CPU, como el relleno de línea Buffers, puertos de carga, o almacenes Buffers.

> *«Los piratas informáticos motivados puedes utilizar las nuevas vulnerabilidades para filtrar datos de información privilegiada de un área de la memoria que los dispositivos de seguridad del hardware consideran fuera de límites. Puede ser implementada en ataques altamente dirigidos que normalmente requerirían privilegios de todo el sistema o una profunda subversión del sistema operativo»,*

> dijo BitDefender.

Estas son las vulnerabilidades derivadas de la ejecución especulativa MDS más reciente en procesadores Intel:

- CVE-2018-12126 – Muestreo de datos de búfer de microarquitectura (MSBDS), también conocido como ataque fallout.
- CVE-2018-12130 – Muestreo de datos de búfer de relleno de microarquitectura (MFBDS), también conocido como Zombieload o RIDL (Carga de datos en vuelo no fiable).
- CVE-2018-12127 – Muestra de datos de puerto de carga microarquitectónica (MLPDS), también parte de la clase de ataques RIDL.
- CVE-2019-11091 – Memoria de muestra de datos de microarquitectura (MDSUM), también parte de la clase de ataques RIDL.

El ataque de fallout es un nuevo ataque de ejecución transitoria que podría permitir que los procesos de usuarios sin privilegios roben información de un componente de microarquitectura previamente inexplotado llamado Store Buffers.

El ataque puede ser utilizado para leer datos que el sistema operativo escribió recientemente y también ayuda a determinar la posición de la memoria del sistema operativo que podría explotarse con otros ataques.

En su ataque de prueba de concepto, los investigadores demostraron cómo se podría utilizar fallout para romper la aleatorización del diseño del espacio de direcciones del kernel (KASLR), y filtrar los datos confidenciales escritos en la memoria por el kernel del sistema operativo.

El ataque ZombieLoad afecta a una amplia gama de computadoras de escritorio, portátiles y computadoras en la nube con generaciones de procesadores Intel lanzadas a partir de 2011 en adelante. Se puede utilizar para leer datos a los que se accedió recientemente o en paralelo en el mismo núcleo del procesador.

ZombieLand no solo funciona en computadoras personales para filtrar información de otras aplicaciones del sistema, sino que también puede ser explotado en máquinas virtuales que se ejecutan en la nube con hardware común.

> *«Además, ZombieLoad no se limita a la ejecución de código nativo, sino que también funciona por medio de los límites de la virtualización. Por lo tanto, las máquinas virtuales pueden atacar no solo al hipervisor, sino también a diferentes máquinas virtuales se ejecutan en un núcleo lógico de hermanos».*
>
> *«Llegamos a la conclusión de que la desactivación de hyperthreading, además de vaciar varios estados de microarquitectura durante los cambios de contexto, es la única solución posible para evitar este ataque extremadamente poderoso»,* dijeron los investigadores.

Los investigadores incluso pusieron a disposición una herramienta para usuarios de Windows y Linux para probar sus sistemas contra los ataques de RIDL y Fallout, así como otras fallas de ejecución especulativa.

También probaron sus explotaciones de prueba de concepto contra las microarquitecturas Intel Ivy Bridge, Haswell, Skylake y Kaby Lake, como se muestra en las demostraciones de video.

Los académicos descubrieron las vulnerabilidades de MDS de la universidad austriaca TU Graz, Vrije Universiteit Amsterdam, la Universidad de Michigan, la Universidad de Adelaida, KU Leuven en Bélgica, el Instituto Politécnico de Worcester, la Universidad de Saarland en Alemania y las firmas de seguridad Cyberius, BitDefender, Qihoo360 y Oracle.

Múltiples investigadores informaron independientemente a Intel sobre las vulnerabilidades de MSD a partir de junio de 2018, pero el gigante tecnológico pidió a todos los investigadores que mantuvieran sus descubrimientos en secreto, algunos por más de un año, hasta que la

compañía pudiera encontrar soluciones para las vulnerabilidades.

Intel lanzó ahora actualizaciones de Microcode Updates (MCU) para corregir las vulnerabilidades de MDS tanto en el hardware como en el software al eliminar todos los datos de los buffers cuando la CPU cruza un límite de seguridad para que los datos no puedan filtrarse ni robarse.

Se recomienda que todos los sistemas operativos, proveedores de virtualización y otros fabricantes de software implementen el parche lo más pronto posible.

Los chips AMD y ARM no son vulnerables a los ataques MDS, e Intel asegura que algunos modelos de sus chips ya incluyen arreglos de hardware contra la falla.

Apple dijo que lanzó una solución para la vulnerabilidad en MacOS Mojave 10.14.5 y las actualizaciones de Safari que se lanzaron antier.

Microsoft también lanzó actualizaciones de software para ayudar a mitigar las vulnerabilidades de MDS. En algunos casos, la compañía dijo que la instalación de las actualizaciones tendrá un impacto en el rendimiento.