Una nueva variante de la vulnerabilidad de fuga de datos en canal lateral, denominada como ZombieLoad V2, también afecta a las CPU Intel más recientes, incluyendo Cascade Lake, que de otra forma es resistente a ataques como Meltdown, Foreshadow y otras variantes de MDS (RIDL y Fallout).

ZombieLoad fue descubierta inicialmente en mayo de este año, y es uno de los tres nuevos tipos de vulnerabilidades de ejecución especulativa de muestreo de datos de microarquitectura (MDS) que afectan a las generaciones de procesadores Intel lanzadas a partir de 2011.

La primera variante de ZombieLoad es un ataque de tipo Meltdown, que se dirige a la lógica del búfer de relleno que permite a los atacantes robar datos confidenciales no solo de otras aplicaciones y del sistema operativo, sino también de máquinas virtuales que se ejecutan en la nube con hardware común.

Ahora, el mismo grupo de investigadores reveló detalles de la segunda variante de la vulnerabilidad, rastreada como CVE-2019-11135, que reside en las Extensiones de Sincronización Transacciones (TSX) de Intel.

Intel TSX proporciona soporte de memoria transaccional en el hardware, con el objetivo de mejorar el rendimiento de la CPU al acelerar la ejecución de software de subprocesos múltiples y anular una transacción cuando se encuentra un conflicto de acceso a la memoria.

Intel se refirió a la vulnerabilidad ZombieLoad v2 como *«Anulación asincrónica de las extensiones de transacciones»,* debido a que la explotación de esta falla requiere un atacante local, con la capacidad de monitorear el tiempo de ejecución de las regiones TSX, para ingerir el estado de la memoria al comparar la ejecución de aborto.

ZombieLoad v2 afecta a computadoras de escritorio, computadoras portátiles y computadoras en la nube que ejecutan cualquier CPU Intel que admita TSX, incluidos los procesadores Core, Xeon y Cascade Lake, la línea de CPU de gama alta de Intel que se

introdujo en abril de 2019.

Parches de microcódigo disponibles

Los investigadores advirtieron a Intel acerca de ZombieLoad v2 el 23 de abril, al mismo tiempo que descubrieron e informaron sobre las otras fallas de MDS que el fabricante de chips solucionó un mes más tarde.

El 10 de mayo, el equipo también informó a Intel que ZomibeLoad V2 funciona contra las líneas más nuevas de las CPU de la compañía, incluso cuando incluyen mitigaciones de hardware contra ataques MDS.

Intel pidió a los investigadores que no revelaran los detalles de la variante 2 hasta ahora, cuando el fabricante de chips presentó parches de seguridad con una actualización de microcódigo que aborda la vulnerabilidad.

La compañía también proporcionó mitigaciones MDS para desarrolladores de sistemas operativos, desarrolladores de máquinas virtuales (VMM), desarrolladores de software que utilizan Intel SGX y administradores de sistemas.

Para obtener más detalles sobre la nueva vulnerabilidad ZombieLoad V2, puedes acceder al documento de investigación original de mayo, que se ha actualizado para la nueva información.

RedHat también lanzó un script con el que los usuarios pueden detectar si su sistema con tecnología Intel también es vulnerable.