Nuevas vulnerabilidades afectan a muchos de los procesadores Intel de los últimos años

El año pasado no fue bueno para Intel por varios motivos –retraso de los 10 nm, falta de producción y problemas de seguridad– y este parece que iba mejorando hasta que ha llegado una nueva tanda de vulnerabilidades.

Están basadas en el abuso de la ejecución especulativa que ya usaran las vulnerabilidades conocidas como Meltdown y Spectre, pero más refinidas. En descargo de Intel, la compañía ya avisó que habría diversas vulnerabilidades relacionadas y por ello ha estado pagando a investigadores para que le ayuden a encontrarlas y parchearlas.

En esta ocasión Intel le ha dado un nombre genérico a tres vulnerabilidades, muestreo de datos de microarquitectura (MDS, *microarchitectural data sampling*) las cuales han sido encontradas tanto por Intel como por tres grupos de investigación que le han dado el nombre de RIDL,

Fallout y ZombieLoad.

Esta vulnerabilidad tiene que ver con los búferes del procesador y cómo gestiona la información que guarda en ellos en lugar de atacar el sistema de caché como se hace en las vulnerabilidades anteriores de Metldown y Spectre. La ejecución especulativa intenta suponer o especular sobre qué instrucciones ejecutar de manera adelantada para ir avanzando trabajo de las instrucciones que se están ejecutando en la línea principal, y en caso de errar no pasaría nada –salvo que hayan fallos de seguridad–.

MDS es similar y afecta a los búferes previos a la caché en los que se deja temporalmente la información extraída de memoria principal antes de escribir esa información en la caché. Pero por la forma de funcionar, pueden dejar información *olvidada* en esos búferes y mediante instrucciones de almacenamiento y carga se puede llevar esa información nuevamente a la memoria principal por programas que aprovechen la vulnerabilidad MDS.

Las buenas noticias para Intel es que la información que se guarda en los búferes no es posible de saber previamente cuál será y por tanto la utilidad de esa información es bastante limitada. Habría que estar continuamente leyendo de los búferes para intentar encontrar una información mínimamente útil. Por ejemplo, los investigadores han tenido que ejecutar en bucle el comando *passwd* en Linux para poder terminar capturando la contraseña, y ciertamente un usuario no va a introducir miles de veces seguidas su contraseña en un equipo.

Según detalla Intel, el muestreo de información de microarquitectura está ya resuelto a nivel de *hardware* en muchos de los procesadores Core de 8.ª y sobre todo los de 9.ª generación así como la 2.ª generación de los Xeon escalables. Se puede consultar el listado de los no afectados en la web de Intel, aunque hay que remitirse a que hay versiones de un mismo procesador que están afectadas y otras que no, indicado

por el número de revisión. Se puede consultar en más detalle en este otro enlace de Intel.

El resto de procesadores de los últimos años, al menos desde los de 2011, tendrán que recibir un parche para evitar ser vulnerables antes estos ataques. Estas vulnerabilidad aparentemente están solo relacionadas con los procesadores de Intel, y por tanto los de AMD y los de arquitectura ARM están a salvo, aunque todavía no se ha podido confirmar al cien por cien.

Fuente: Ars Technica.