MIT encuentra una solución a las vulnerabilidades Meltdown y Spectre

Las vulnerabilidades en los procesadores Meltdown y Spectre han sido una verdadera pesadilla a lo largo de este año. El mayor afectado, Intel, ha desarrollado todo tipo de soluciones para mitigarlas, pero meses después, incluso las últimas generaciones de chips que han llegado al mercado no son completamente seguras y el parcheo para modelos anteriores afecta al rendimiento en más o menos grado.

El CERT (Computer Emergency Response Team), el centro de respuesta a incidentes de seguridad en tecnologías de la información y referente absoluto en ciberseguridad, emitió unas declaraciones sobre Meltdown y Spectre que se ha cumplido punto por punto: “Debido al hecho de que la vulnerabilidad existe en la arquitectura de la CPU en lugar de el software, los parches no pueden abordarla plenamente en todos los casos.

Para eliminar la vulnerabilidad por completo, será necesario reemplazar la CPU afectada“.

Y no en una generación sino en las siguientes. Intel (y otros productores como AMD y ARM) tendrán que rediseñar ciertas características de sus futuros procesadores para superar finalmente Meltdown y Specter.

Para entender el problema, debemos comprender cual es la solución vía software que están proporcionando los proveedores para mitigar los ataques bajo estas vulnerabilidades y que tienen que ver con la propia arquitectura de los chips. Los procesadores no separan por completo los procesos clave que tienen acceso al kernel del sistema operativo de aquellos con privilegios bajos y de poca confianza (como los de muchas aplicaciones), por lo que un atacante podría aprovechar esta función para que el procesador le anticipe datos que no debería gracias a la ejecución especulativa y conseguir cualquier dato del equipo en cuestión.

De ahí que solucionar esta vulnerabilidad vía software (al menos para Meltdown) implica necesariamente separar los procesos del usuario de la memoria del kernel y con ello variar el funcionamiento del procesador, que en el caso de Intel (y también los de otros fabricantes compatibles) gana rendimiento precisamente con un tipo de técnicas de elevación de privilegios que en las últimas horas ha sido duramente criticadas por el creador de Linux, Linus Torvalds.

Propuesta del MIT para Meltdown y Spectre

Se imponen cambios en la misma arquitectura y los investigadores del MIT (Instituto de Tecnología de Massachusetts) han desarrollado una forma de particionar y aislar los cachés de memoria con “dominios de protección” y evitar la explotación de la “ejecución especulativa”.

A diferencia de la Tecnología de asignación de caché (CAT) de

Intel, la tecnología de MIT, llamada DAWG (Guardia asignada dinámicamente) no permite los ataques en esos dominios de protección. Esto es importante, porque estas vulnerabilidades aprovechan los “ataques de sincronización de caché” y pueden obtener acceso a datos confidenciales y privados.

DAWG funciona de manera similar a CAT y no requiere muchos cambios en el sistema operativo del dispositivo, lo que hace que sea tan fácil de instalar en una computadora afectada como la solución de microcódigo que se ha propuesto para Meltdown. Según los investigadores, la nueva técnica “establece límites claros en los lugares donde se debe y no se debe compartir, para que los programas con información confidencial puedan mantener esa información razonablemente segura”.

Aunque el DAWG no puede prevenir cada ataque especulativo, los investigadores dicen estar trabajando para mejorar la mayoría de ellos. Otro tema importante es que esta tecnología no solo podría ayudar a proteger las computadoras normales, sino también las infraestructuras vulnerables de la nube.

Interesante, aunque conviene recalcar que la técnica del MIT contra Meltdown y Spectre es un diseño para los chips del futuro no para los presentes para los que solo se puede mitigar al localizarse en la propia arquitectura de los chips.

Fuente: muyseguridad.