MELTDOWN y SPECTRE: Qué son y cómo cuidarse

Introducción

Recientemente se publicó información sobre problemas de diseño de CPUs modernas que hacen posible el robo de información en prácticamente cualquier computadora actual, siempre y cuando se pueda ejecutar código arbitrario en ella. En esta nota contamos de qué se trata y cómo protegerse.

Ejecución especulativa

La ejecución especulativa es una estrategia de hardware que la mayoría de los procesadores actuales utiliza para mejorar el desempeño de los programas, que consiste en que al llegar a una parte del programa que requiere tomar una decisión, el procesador "apuesta" a que el resultado de la decisión es uno, y adelanta trabajo como si ya estuviera yendo por ese camino; si acertó, tiene parte del trabajo hecho, y si se equivocó todo el trabajo adelantado se descarta y es como si hubiera estado esperando al resultado sin hacer nada. [Nota: esta explicación evita deliberadamente hablar del pipeline. Si usted sabe qué es el pipeline, puede ir directamente a las referencias al final de la nota]

El problema

Lo que descubrieron diversos equipos de investigadores en seguridad en Junio (ver papers en la sección Referencias) es que **no todos** los efectos del trabajo adelantado desaparecían, y por métodos más o menos indirectos un proceso cualquiera podía acceder a memoria a la que en principio el sistema operativo no le permitía acceder (memoria de otros procesos, o incluso del sistema operativo propiamente dicho).

Los ataques

Hay dos ataques distintos que se pueden hacer para abusar de esta capacidad: los creadores los bautizaron MELTDOWN y SPECTRE [link]. MELTDOWN es exclusivo de los procesadores de Intel, y se encuentra en prácticamente todos, mientras que SPECTRE afecta a Intel, AMD, ARM y básicamente cualquier procesador que realice ejecución especulativa. Otra diferencia es que MELTDOWN tiene solución a través del sistema operativo, mientras que SPECTRE no tiene mitigación conocida (aunque es más difícil de llevar a cabo). SPECTRE funciona independientemente del sistema operativo que se esté utilizando; MELTDOWN funciona en cualquier sistema operativo que no tenga la mitigación específica para impedirlo. Entendemos que tanto Microsoft como Linux tienen parches desarrollados, y estarían siendo distribuidos en las próximas horas (para Linux varía según la distribución).

Qué efectos tienen

Los dos ataques permiten a un proceso leer el contenido de memoria a la que en principio no deberían tener acceso, lo que en términos de seguridad es muy grave: los efectos pueden ir desde leer las contraseñas que estén en memoria (por ejemplo, si guardamos contraseñas en el navegador y le pedimos que las muestre) hasta derrotar medidas de protección del sistema operativo. Por supuesto, para llevar a cabo el ataque hace falta estar corriendo un proceso en la máquina víctima, lo que no debería ser común… salvo que estemos utilizando un navegador de internet. Cada vez que entramos en un sitio Web, éste descarga y ejecuta una variedad de programas que pueden formar parte o bien del sitio Web, o bien de bibliotecas utilizadas por el sitio Web, o incluso de avisos publicitarios (que la empresa que los envía usualmente no

verifica). Así que en realidad estamos descargando y ejecutando código de fuentes desconocidas prácticamente todo el tiempo.

Qué se puede hacer

Recomendaciones básicas (las primeras se recomiendan siempre, no sólo en este caso):

– No descargar programas de fuentes desconocidas o poco confiables.

– Mantener actualizado el sistema operativo.

– No conectarse a redes WiFi “libres”.

– No visitar páginas de legitimidad “cuestionable”.

– Usar un ad blocker (inhabilitar JavaScript es más seguro, pero la mayoría de los sitios dejan de funcionar).

Referencias

1. Descripción y links.

2. Paper de MELTDOWN.

3. Paper de SPECTRE.

Post de Google Project Zero.