

Perturbadora ejecución especulativa

Parece que 2018 no quiere pasar desapercibido. Se publican dos nuevas vulnerabilidades de seguridad a nivel de hardware y más en concreto de diseño de los microprocesadores, con probabilidad se trate de la mayor vulnerabilidad de la historia. Meltdown y Spectre se aprovechan de una función de rendimiento de las CPU modernas llamada ejecución especulativa, desde el CERT (Computer emergency response team) sugieren sustituir todos los microprocesadores afectados (muerto el perro se acabó la rabia), una solución de lo más radical que supondrá un importante desembolso económico.

Meltdown afecta a cualquier procesador Intel posterior a 1995, rompe el aislamiento más fundamental entre las aplicaciones de usuario y el sistema operativo. Este ataque permite que un programa acceda a la memoria, y por lo tanto también a los secretos, de otros programas y del sistema operativo. Si el equipo tiene un procesador vulnerable y ejecuta un sistema operativo sin parcheo, no es seguro trabajar con información confidencial sin la posibilidad de que se filtre la información. Esto se aplica tanto a los ordenadores personales como a la infraestructura cloud.

La vulnerabilidad fue denominada Meltdown (CVE-2017-5754) o "carga irregular de información en caché", básicamente lo que hace es derretir las barreras de seguridad que normalmente coloca el hardware. Los fabricantes del hardware y el software afectados tuvieron conocimiento del problema el 28 de julio de 2017.

Spectre afecta a los procesadores AMD, ARM e Intel, rompe el aislamiento entre diferentes aplicaciones. Permite a un atacante engañar a los programas libres de errores, que siguen las mejores prácticas, para que filtren sus secretos. De hecho, las comprobaciones de seguridad de dichas mejores prácticas aumentan la superficie de ataque y pueden hacer que las aplicaciones sean más susceptibles a Spectre. Spectre es más difícil de explotar que Meltdown, pero también es más difícil de mitigar.

La vulnerabilidad fue denominada "Spectre" (espectro) que engloba dos técnicas diferentes de explotación conocidas como CVE-2017-5753 o «baiting» de la comprobación de límites de memoria y CVE-2017-5715 o «injection» en el objetivo del predictor de saltos. Puesto que no es fácil de corregir, será algo que nos persiga durante mucho tiempo (como un fantasma). Los fabricantes del hardware afectado tuvieron conocimiento del problema el 1 de junio de 2017.

Ambas vulnerabilidades se hicieron públicas el 3 de enero de 2018. Más información: Meltdown y Spectre y Consejo Europeo de Investigación

La tecnología actual depende de tres multinacionales INTEL, AMD y ARM y no disponemos de alternativas. Los gobiernos deberían tomarse en serio la independencia tecnológica.