Perturbadora ejecución especulativa

Parece que 2018 no quiere pasar desapercibido. Se publican dos nuevas vulnerabilidades de seguridad a nivel de hardware y mÃ¡s en concreto de diseÃ±o de los microprocesadores, con probabilidad se trate de la mayor vulnerabilidad de la historia. Meltdown y Spectre se aprovechan de una funciÃ³n de rendimiento de las CPU modernas llamada ejecuciÃ³n especulativa, desde el CERT (Computer emergency response team) sugieren sustituir todos los microprocesadores afectados (muerto el perro se acabÃ³ la rabia), una soluciÃ³n de lo mas radical que supondrÃ-a unÂ importante desembolso econÃ³mico.

Meltdown afecta a cualquier procesador Intel posterior a 1995, rompe el aislamiento mÃ¡s fundamental entre las aplicaciones de usuario y el sistema operativo. Este ataque permite que un programa acceda a la memoria, y por lo tanto tambiÃ©n 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 informaciÃ³n confidencial sin la posibilidad de que se filtre la informaciÃ³n. 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 informaciÃ³n en cachÃ©", bÃ¡sicamente 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 engaÃ±ar a los programas libres de errores, que siguen las mejores prÃ¡cticas, para que filtren sus secretos. De hecho, las comprobaciones de seguridad de dichas mejores prÃ¡cticas aumentan la superficie de ataque y pueden hacer que las aplicaciones sean mÃ¡s susceptibles a Spectre. Spectre es mÃ¡s difÃ-cil de explotar que Meltdown, pero tambiÃ©n es mÃ¡s difÃ-cil de mitigar.

La vulnerabilidad fue denominada "Spectre" (espectro) que engloba dos tÃ©cnicas diferentes de explotaciÃ³n conocidas como CVE-2017-5753 o â€œbaipÃ¡s de la comprobaciÃ³n de lÃ-mites de memoriaâ€• y CVE-2017-5715 o â€œinyecciÃ³n en e objetivo del predictor de saltosâ€•. Puesto que no es fÃ¡cil de corregir, serÃ¡ 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 pÃºblicas el 3 de enero de 2018. MÃ¡s informaciÃ³n: Meltdown y Spectre y Consejo Europeo de InvestigaciÃ³nÂ
La tecnologÃ-a actual depende deÂ tres multinacionales INTEL, AMD y ARM yÂ no disponemos de alternativas. Los gobiernos deberÃ-an tomarse en serio la independencia tecnolÃ³gica.