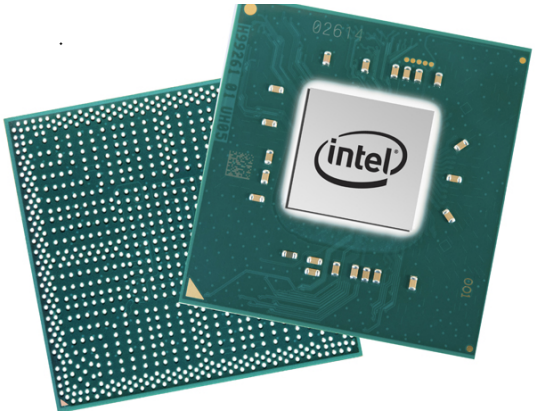
# Intel dice que todos los procesadores, también de otras marcas, presentan fallos

Ayer salía la noticia sobre el primera gran fallo de seguridad identificado durante este año 2018: todos los procesadores fabricados por Intel en los últimos diez años llegan con unos fallos de seguridad que permitirían a los ciberdelincuentes acceder a la información de nuestras computadoras, también  a la más crítica, como contraseñas. Y que el parche en el que trabaja la empresa ralentizaría de forma muy considerable los equipos y los dejaría muy por debajo de su rendimiento.




Pues bien, hoy Intel ha emitido un comunicado en el que afirma que procesadores de otras marcas también presentan el mismo problema. Según el comunicado, "lo es cierto lo que indican unos informes recientes que afirman que estas vulnerabilidades son fruto de un "error" o de un "fallo" y que sólo aparecen en productos de Intel. Basándonos en estudios realizados hasta la fecha, muchos tipos de dispositivos informáticos, con **procesadores y sistemas operativos de numerosos y diferentes suministradores, son susceptibles de verse afectados por estas vulnerabilidades"**

La firma de chips ha dicho estar trabajando con otras empresas del sector como **AMD, ARM Holdings y con varios suministradores de sistemas operativos**, "para desarrollar un mecanismo para resolver este problema en todo el sector de forma inmediata y constructiva. Intel ha comenzado a proporcionar actualizaciones de software y firmware para minimizar estas vulnerabilidades", pero no da grandes especificaciones sobre qué es lo que hará para remediar tan enorme problema en la seguridad de los ciudadanos del mundo.

También afirman desde la empresa que "al contrario de lo que afirman algunos informes, cualquier impacto en el rendimiento dependerá de la carga de trabajo que se realice y, para el usuario medio de ordenadores, no debería ser considerable y se mitigará con el tiempo".

Mientras aparezca una solución, la multinacional recomienda a los usuarios consultar con su proveedor del sistema operativo o con u fabricante del sistema y realizar las actualizaciones disponibles lo antes posible.  "El cumplimiento de buenas prácticas en seguridad para proteger los sistemas contra cualquier malware en general también ayudará a proteger a los usuarios contra una posible vulnerabilidad hasta que se encuentren disponibles las actualizaciones correspondientes", concluye el comunicado.

## Red Hat: el exploit tiene tres rutas de ataque

Por su parte, **Red Hat Product Security** ha recordado que las vulnerabilidades que afectan a los procesadores y sistemas operativos en las principales plataformas de hardware, incluyen las de la

familia **x86** (circuito integrado auxiliar de Intel y AMD), **POWER 8, POWER 9, System z** y **ARM**, y que esta podría permitir el acceso de lectura no autorizado a la memoria.

"El exploit **tiene tres rutas de ataque únicas que podrían permitir a un atacante ejecutar un "ataque de canal lateral"** para eludir las protecciones y así leer la memoria del dispositivo", dicen desde Red Hat que hacen hincapié en que este problema es de "gravedad importante". Los tres vulnerabilidades y exposiciones comunes para este problema son:

- CVE-2017-5754 (Meltdown) es el más grave de los tres. Este exploit **utiliza la speculative cache loading para permitir a los atacantes leer los contenidos de la memoria**. Este problema se corrige con parches de kernel.

- CVE-2017-5753 (Spectre) es un Bounds-checking exploit durante el branching. Este problema se corrige con un parche de kernel.

- CVE-2017-5715 (Spectre) es un branching poisoning attack que puede conducir a la pérdida de datos. Este ataque permite que un huésped virtualizado lea la memoria del host system. Este problema se corrige con microcódigo, junto con las actualizaciones de kernel y la virtualización tanto para el software huésped y host de virtualización.