Intel: los informes de la vulnerabilidad de sus chips son incorrectos y afecta a más fabricantes

Hace menos de un día, The Register dio la voz de alarma sobre una vulnerabilidad que afecta a cómo maneja la memoria virtual los procesadores de Intel. Esto podía llevar a que un pirata pueda acceder a zonas de memoria reservadas al núcleo del sistema operativo, y por tanto se puede considerar como muy grave. A partir de ahí, debido a que no se ha dado mucha más información, o más información que sea veraz y contrastada, han surgido todo tipo de conjeturas. Incluida, la de que los PC de los hogares van a perder hasta un 35 % de rendimiento.

En estos casos hay que ser cautos, aunque los mercados han hecho ascender las acciones de AMD, supuestamente no afectada, y ha hecho descender las de Intel. La compañía no ha tenido más remedio que emitir un comunicado para aclarar ciertos puntos antes de que más noticias falsas inunden internet sobre este tema.

Según lo que deja entender Intel en la siguiente declaración, el problema también afecta a los procesadores de AMD así como los que están basados en la arquitectura ARM, como los usados en los teléfonos inteligentes.

Intel y otras empresas tecnológicas han sido avisadas de una nueva investigación de seguridad que describe métodos de análisis de programación que, cuando son usados con fines malintencionados, tienen el potencial de recolectar indebidamente información sensible de computadoras que están funcionando correctamente como han sido programadas. Intel cree que estas vulnerabilidades no tienen el potencial de corromper, modificar o borrar información.

Noticias recientes han indicados que estas vulnerabilidades están causadas por un error o defecto y que son únicos a los productos de Intel. Es falso. Basándonos en los análisis hasta ahora, muchos tipos de computadoras –afectando a los procesadores de muchos vendedores así como diferentes sistemas operativos– son susceptibles de sufrir esta vulnerabilidad.

Intel está comprometida con la seguridad de sus productos y sus clientes, y está trabajando estrechamente con muchas empresas de tecnología diferentes, incluyendo AMD, ARM Holdings y otros vendedores de sistemas operativos, para desarrollar una solución consensuada por la industria para resolver este problema lo más rápidamente posible.

Intel ha comenzado a proporcionar actualizaciones de software y hardware para mitigar estas vulnerabilidades. Al contrario de lo que se indica en las noticias, cualquier impacto de rendimiento varían según el tipo de carga y, para el usuario doméstico medio, no debería notarse y se reducirá con el tiempo.

Intel está comprometida con la buena práctica de la industria de revelar de una forma responsable los potenciales fallos de seguridad, que es por lo que Intel y otras empresas habíamos

planeado revelar el problema la próxima semana cuando estuvieran disponibles más actualizaciones de hardware y software. Sin embargo, Intel está realizando esta declaración hoy debido a los informes imprecisos de los medios de comunicación.

Fuente: geektopia.