A pesar de los parches lanzados para reparar las vulnerabilidades en procesadores Intel y AMD, se ha dado a conocer la existencia de Spectre 1.1 y Spectre 1.2, dos nuevos fallos de seguridad que afectan a los procesadores.

Spectre vuelve a atacar a Intel con dos variantes, por su parte, la compañía de microprocesadores dice que trabaja en mejores actualizaciones. Spectre 1.1 y Spectre 1.2 afectan al proceso de ejecución especulativa, integrado en la mayoría de los nuevos procesadores.

Estas dos nuevas variantes afectan a los chips de ARM, Intel y AMD, ya que muchos de los procesadores modernos utilizan una rama de ejecución especulativa. Este técnica es muy recurrida para el incremento del rendimiento de los procesadores y es en lo que se basan estas dos vulnerabilidades.

Spectre 1.1 es similar a la vulnerabilidad publicada en enero y también es parecida a la variante Spectre V4 que se publicó a finales de mayo. Cuando se aprovecha este fallo, el atacante puede utilizar la ejecución especulativa para cerrar un desbordamiento de buffer de la caché de almacenamiento del procesador. Con esto, podría escribir y ejecutar código malicioso en direcciones de memoria.

En el caso de Spectre 1.2, la vulnerabilidad permitiría escribir en algunos sectores de la memoria del procesador que normalmente están marcados como *«sólo lectura»*. Esto afectaría a las funciones de seguridad en las que el hardware ejecuta código, por lo que dejarían de ser efectivas.