Descubren un fallo irreparable en el procesador oculto que usan dispositivos electrónicos, coches y aviones

Uno de los componentes más importante a nivel de hardware en cualquier dispositivo electrónico es el procesador, ya que es el encargado de dar vida al propio dispositivo.

La velocidad a la que es capaz de procesar las acciones un dispositivo, así como su conjunto de habilidades dependen en gran medida de las características y prestaciones del procesador, de ahí su gran importancia. Cuando hablamos de procesador o SoC, lo primero que nos puede venir a la cabeza es el chip encargado de ejecutar las órdenes en ordenadores, teléfonos móviles y otros dispositivos electrónicos, pero también tienen una gran importancia en otros dispositivos industriales, militares, de automoción o incluso aviación.

De esta manera, un fallo en el procesador puede afectar al funcionamiento general del dispositivo. Estos fallos pueden clasificarse como fallos a nivel de software o hardware y como tal, pueden tener una u otra solución. Si se detecta un fallo en el firmware o software encargado de controlar y manejar el componente hardware, la solución pasa por actualizar ese software sin que sea necesario alterar nada a nivel físico.

Sin embargo, si el fallo está a nivel de hardware, entonces la solución no es tan sencilla, ya que el componente deberá ser sustituido o modificado. La solución también se puede complicar con la unión de varios problemas a nivel de software, tal y como ha ocurrido con uno de los procesadores del fabricante Xilinx.

Detectan un fallo irreparable en un procesador del fabricante Xilinx

Un grupo de investigadores de seguridad han descubierto dos fallos importantes de seguridad en procesadores de dicho fabricante, concretamente en el SoC Zynq UltraScale +. Procesador que podemos encontrar en todo tipo de dispositivos, tanto de electrónica de consumo como automoción, militar o aviación, puesto que incluye sistema en chip (SoC), sistema multiprocesador en chip (MPSoC), así como sistema en chip de radiofrecuencia (RFSoC). Uno de estos fallos podría ser reparado por una actualización a nivel de software, sin embargo, el otro sería irreparable.

El primero de ellos es una vulnerabilidad en el modo de inicio seguro, ya que no cifra correctamente los metadatos del proceso de arranque realizado por la ROM y los deja expuestos a posibles modificaciones con malas intenciones. De esta forma, un atacante podría hacer que se ejecutase código malicioso.

Sin embargo, un segundo fallo detectado en el análisis de la

tabla de particiones también permitiría la ejecución de código malintencionado. A diferencia con el anterior error, este último sería irreparable dado que, un atacante podría evitar que se instalase cualquier parche que dé solución a este error si explotan la vulnerabilidad anterior.

Por suerte, los atacantes únicamente podrían explotar estos fallos de seguridad teniendo acceso físico al dispositivo. No obstante, Xilinx ya ha procedido a modificar los manuales de estos chips para que los proveedores de equipos o dispositivos que utilizan SoCs Zynq UltraScale + sepan usar el modo de arranque seguro HWRoT (Hardware Root of Trust), que en este caso no se ha visto afectado por estos fallos.

Fuente: adslzone.