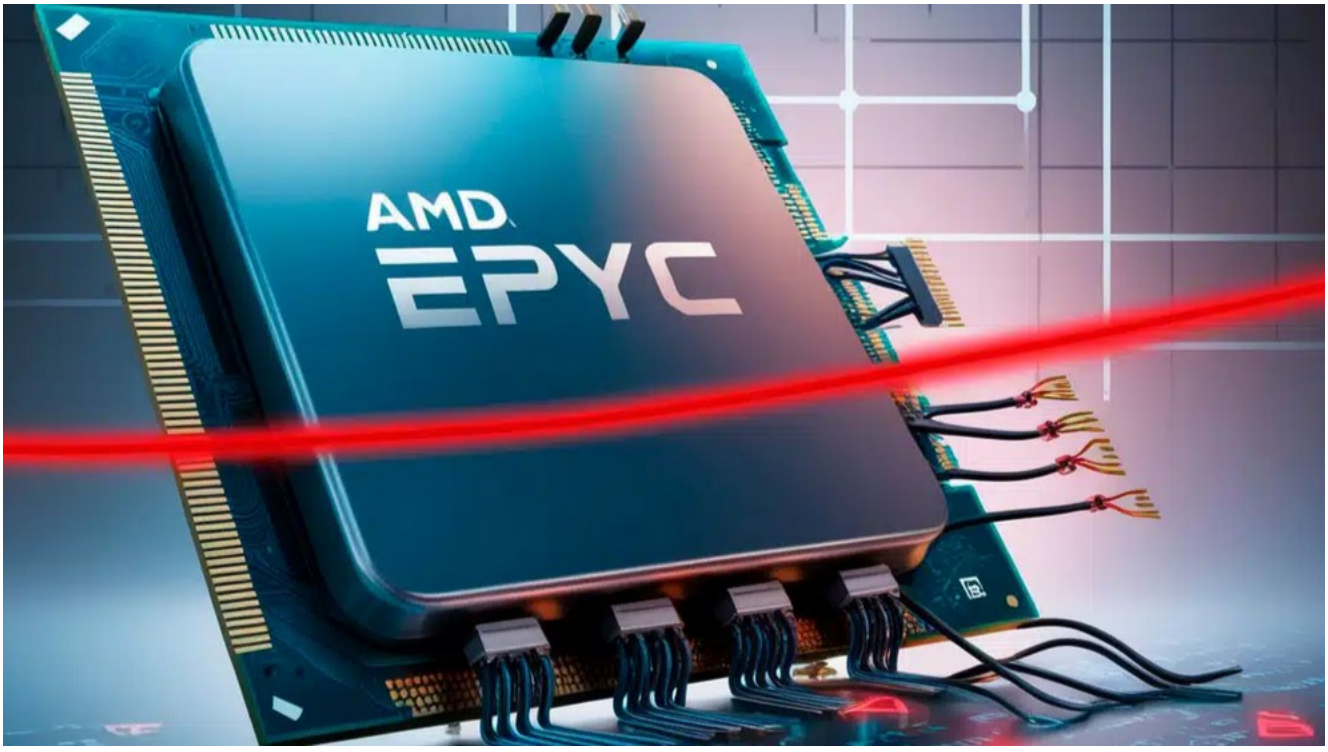
Google da los detalles completos de la vulnerabilidad «EntrySign» de alta gravedad que afecta a CPU AMD Zen 1 a Zen 4

Aunque los procesadores puedan parecer muy seguros, lo cierto es que estos también pueden ser víctima de atacantes y cibercriminales.

Mientras existan brechas de seguridad y exploits que puedan aprovechar para entrar al sistema esto seguirá pasando y por desgracia, no hay ningún sistema que evite esto al 100%. Solemos ver noticias de vulnerabilidades que afectan a CPU de ambas compañías, pero ahora han sido los investigadores de **Google** los que han dado los detalles de una **vulnerabilidad** de alta gravedad llamada **EntrySign que afecta a casi todas las CPU Zen**.



Cada cierto tiempo tanto Intel como AMD suelen publicar informes de seguridad donde se revela todo lo que está ocurriendo en términos de vulnerabilidades en su hardware. Aquí también debemos incluir empresas como NVIDIA, aunque en este caso son bastante menos frecuentes y suelen ocurrir a nivel de software y drivers. Los procesadores, en cambio, pueden acabar con decenas de vulnerabilidades descubiertas en cuestión de un par de años y algunas de ellas son de muy alta gravedad.

Google da todos los detalles de la vulnerabilidad EntrySign que afecta a las CPU AMD Zen

El mes pasado, los investigadores de Google revelaron que hay una vulnerabilidad de seguridad grave que afecta a las CPU AMD Zen 1, Zen 2, Zen 3 y Zen 4. Aunque Google avisó a AMD en septiembre de 2024, la compañía no la arregló incluso meses después de la advertencia. Se trata de una vulnerabilidad de firma de microcódigo que permite instalar parches de microcódigo maliciosos que comprometen la seguridad. La compañía prometió que darían más detalles sobre esta vulnerabilidad el 5 de marzo y ahora tenemos un informe completo.

Google ha revelado que el nombre de esta vulnerabilidad que afecta a CPU Zen es EntrySign (CVE-2024-56161) . Esta permite a los atacantes eludir el sistema de verificación de firmas criptográficas de AMD que se encargan de proteger el microcódigo. Este es importante en las CPU x86, debido a que es la única forma de actualizar y corregir problemas críticos que no requiere sustituir por otra pieza de hardware. A pesar de que estas actualizaciones están protegidas con cifrado y firmas digitales, con este exploit se puede saltar eso y efectivamente se pueden instalar parches no seguros.

Google demuestra como es posible usar microcódigo personalizado con la herramienta Zentool

Esta vulnerabilidad ocurre debido a que AMD usa AES-CMAC como función hash en la verificación de firmas en lugar de optar por emplear un algoritmo hash criptográfico más seguro. Los investigadores de Google descubrieron que AMD empleaba la clave de ejemplo de la documentación del NIST (2b7e1516 28aed2a6 abf71588 09cf4f3c) en varias de sus generaciones de CPU, por lo que aquí no pensó que podría acabar con falsificaciones de firmas.

Para poder demostrar la teoría, los investigadores desarrollaron Zentool una herramienta que permite examinar, crear, firmar y cargar parches de microcódigo personalizados. Tras esto decidieron modificar la instrucción RDRAND para que esta de un valor de 4 en lugar de números aleatorios y efectivamente funcionaba. Aunque eso sí, para que un atacante pueda aprovechar la vulnerabilidad necesita privilegios a nivel de kernel y tendrá que volver a ejecutarlos cada vez que se inicia el ordenador afectado. En caso de que tengas curiosidad sobre Zentool, los investigadores la han compartido en GitHub y por otro lado, tienes el artículo técnico completo en Bug Hunters.

Fuente: elchapuzasinformatico.