Recientemente se ha descubierto una vulnerabilidad de seguridad en los procesadores basados en la arquitectura Zen 2 de AMD que podría ser objeto de explotación para obtener información confidencial como contraseñas y claves de cifrado.

El fallo, bautizado como Zenbleed y registrado como CVE-2023-20593 (con una puntuación CVSS de 6.5), fue descubierto por Tavis Ormandy, investigador de Google Project Zero. Esta falla permite la extracción de datos a una velocidad de 30 kb por núcleo, por segundo.

Este problema es parte del grupo más amplio de debilidades conocidas como ataques de ejecución especulativa, los cuales aprovechan la técnica ampliamente utilizada en las CPUs modernas para acceder a claves criptográficas desde los registros de la CPU.

> En un comunicado, AMD explicó que *«bajo circunstancias microarquitectónicas específicas, un registro en las CPUs «Zen 2″ podría no escribirse correctamente a 0, lo que podría permitir que un atacante potencialmente acceda a información sensible».*

Es importante destacar que el ataque incluso podría ser llevado a cabo a través de JavaScript en un sitio web, lo que obviaría la necesidad de acceso físico al ordenador o servidor. De hecho, la compañía Cloudflare ha señalado esta posibilidad.

> Los investigadores de Cloudflare, Derek Chamorro e Ignat Korchagin, señalaron que *«Las operaciones vectorizadas pueden ejecutarse con gran eficiencia utilizando los registros YMM. Estas operaciones son especialmente beneficiosas para las aplicaciones que manejan grandes volúmenes de datos, pero lamentablemente también se han convertido en un objetivo creciente para actividades maliciosas*«.

> *«Este tipo de ataque se basa en la manipulación de los archivos de registro para*

> *forzar un comando mal predicho. Dado que estos archivos de registro son compartidos por todos los procesos que se ejecutan en el mismo núcleo físico, este exploit permite interceptar incluso las operaciones más fundamentales del sistema al monitorear los datos que se transfieren entre la CPU y el resto de la computadora»*.

Aunque no hay evidencia de que esta vulnerabilidad se haya aprovechado en la vida real, es crucial aplicar las actualizaciones de microcódigo tan pronto estén disponibles a través de los fabricantes originales (OEMs) para mitigar cualquier riesgo potencial.