Un grupo de investigadores reveló detalles de una nueva vulnerabilidad que afecta a las CPU de Intel, y que permite a los hackers obtener claves de cifrado y otra información confidencial de los procesadores.

Nombrada como AEPIC Leak, la vulnerabilidad es la primera de su tipo en divulgar arquitectónicamente datos confidenciales de una forma similar a una *«lectura de memoria no inicializada en la propia CPU».*

> *«A diferencia de los ataques de ejecución transitoria como Meltdown y Spectre, AEPIC Leak es u error arquitectónico: los datos confidenciales se divulgan directamente sin depender de ningún canal lateral (ruidoso)»,* dijeron los investigadores.

El estudio fue realizado por investigadores de la Universidad Sapienza de Roma, la Universidad Tecnológica de Graz, Amazon Web Services y el Centro CISPA Helmholtz para la Seguridad de la Información.

La vulnerabilidad (CVE-2022-21233, puntuación CVSS: 6.0), que afecta a las CPU con microarquitectura Sunny Cover, tiene su origen en un componente denominado Controlador de Interrupción Programable Avanzado (APIC), que proporciona un mecanismo para manejar y enrutar señales de interrupción de hardware en una forma escalable.

> *«La exploración del espacio de direcciones de E/S en las CPU Intel basadas en la microarquitectura Sunny Cover, reveló que los registros asignados en memoria del controlador de interrupción programable avanzado (APIC) local no se inicializaron correctamente»*, dijeron los investigadores.

> *«Como resultado, la lectura arquitectónica de estos registros devuelve datos*

> *obsoletos de la microarquitectura. Cualquier dato transferido entre L2 y el caché de último nivel se puede leer por medio de estos registros».*

AEPIC Leak se dirige específicamente a los sistemas que utilizan el entorno de ejecución confiable (TEE) de Intel conocido como Software Guard eXtensions (SGX), lo que provoca la fuga de claves AES y RSA de enclaves seguros que se ejecutan en el mismo núcleo de CPU físico con una tasa de éxito del 94% y 74% respectivamente.

> *«Al proteger el código y los datos seleccionados de la modificación, los desarrolladores pueden dividir su aplicación en enclaves reforzados o módulos de ejecución confiables para ayudar a aumentar la seguridad de la aplicación»*, explicó Intel sobre las garantías de seguridad que ofrece SGX.

La vulnerabilidad, en pocas palabras, rompe las garantías antes mencionadas, lo que permite que un atacante con permisos ejecute código nativo privilegiado en una máquina de destino para extraer las claves privadas, y lo que es peor, derrotar la atestación, una piedra angular de las primitivas de seguridad usadas en SGX para garantizar la integridad de códigos y datos.

En respuesta a los hallazgos, Intel lanzó actualizaciones de firmware y describió el problema como una vulnerabilidad de gravedad media relacionada con el aislamiento inadecuado de los recursos compartidos, lo que lleva a la divulgación de información a través del acceso local.

También cabe mencionar que, desde entonces, Intel dejó de admitir SGX para las CPU de sus clientes, con una letanía de métodos de ataque que plagan la tecnología, incluidos SGX-ROP, MicroScope, Plundervolt, Load Value Injection, SGAxe y VoltPillager.

El ataque de canal lateral SQUIP afecta a las CPU de AMD

El desarrollo se produce cuando los investigadores demostraron cuál es el primer ataque de canal lateral (CVE-2021-46778) en las colas del programador que afecta a las microarquitecturas AMD Zen 1, Zen 2 y Zen 3 de las que un adversario podría abusar para recuperar claves RSA.

El ataque, cuyo nombre en código es SQUIP (abreviatura de Scheduler Queue Usage via Interference Probing), implica medir el nivel de contención en las colas del programador para obtener potencialmente información confidencial.

No se han publicado actualizaciones de seguridad para parchear la línea de ataque, pero el fabricante de chips recomienda que *«los desarrolladores de software empleen las mejores prácticas existentes, incluyendo los algoritmos de tiempo constante y eviten los flujos de control dependientes de secretos cuando corresponda».*