AMD informó que planea lanzar actualizaciones de firmware para corregir errores que afectan a algunas de sus computadoras portátiles y sistemas integrados.

Los tres errores, a los que AMD se refiere como «SMM Callout», permiten a los hackers tomar el control del firmware UEFI de CPUs AMD e inherentemente, de toda la computadora.

AMD dijo que las vulnerabilidades afectan una pequeña fracción de las CPU de la Unidad de Procesamiento Acelerado (APU) lanzadas entre 2016 y 2019.

Los procesadores AMD APU, anteriormente conocidos como AMD Fusion, son microprocesadores pequeños de 64 bits que incluyen una unidad central de procesamiento (CPU) y unidad de procesamiento de gráficos (GPU) en el mismo dado de silicio.

La noticia sobre estos tres errores se dio a conocer el 13 de junio, cuando un investigador de seguridad llamado Danny Odler, publicó un artículo en Medium que detallaba uno de los tres errores de SSM Callout, que ya estaba parcheado.

Odler dijo que las vulnerabilidades afectan un área de procesadores AMD conocida como SMM, que significa Modo de Administración del Sistema, una capa que se encuentra en el nivel más profundo dentro de algunos tipos de procesadores AMD.

El SSM es una parte del firmware UEFI de la CPU, y el código SMM generalmente se emplea para administrar funciones relacionadas con hardware, como la administración de energía, la suspención del sistema, las hibernaciones, emulaciones de dispositivos, errores de memoria y las funciones de seguridad de la CPU.

Debido a su objetivo de mantener la CPU funcionando e interactuando con los componentes de hardware adyacentes, el código SMM se ejecuta con el más alto nivel de privilegios en una computadora, teniendo el control total sobre el núcleo del sistema operativo y los hipervisores. En otras palabras, el SMM se ejecuta en el nivel más profundo del anillo de la CPU, el Anillo-2.

Entonces, cualquier atacante que logre infectar el SSM generalmente tiene control total no solo del sistema operativo, sino también del hardware de una computadora.

La semana pasada, Odler dijo que encontró tres errores en el módulo SMM de AMD, que pueden permitirle la implantación de código malicioso dentro de SMRAM (la memoria interna de SMM) y ejecutarlo con los privilegios de SMM.

> *«La ejecución de código en SMM es un juego terminado para todos los límites de seguridad como SecureBoot, Hypervisor, VBS, Kernel y más»*, dijo el investigador.

La explotación de los errores de SMM Callout requiere acceso físico al dispositivo o malware en la computadora de la víctima que puede ejecutar código malicioso con privilegios de administrador.

Aunque estas condiciones para un ataque de SMM Callout parecen prohibitivas, no han detenido a los desarrolladores de rootkits en los últimos 15 años, por lo que no deja de ser una posibilidad.

Odler dijo que informó los tres errores a AMD a inicios de abril, y la compañía ya había lanzado parches para el primer error, rastreado como CVE-2020-14032.

Otros dos errores permanecen sin parchear, pero en un aviso de seguridad publicado esta semana, AMD dijo que planea tener los parches de AGESA listos para fin de mes.

AGESA (AMD Generic Encapsulated Software Architecture) es el nombre en clave de AMD para el firmware UEFI (Interfaz de Firmware Extensible Unificada).

Cuando las actualizaciones de AGESA estén listas con los parches para las otras dos vulnerabilidades de SMM Callout, AMD dijo que compartirá el firmware con los proveedores de placas base y los fabricantes de sistemas integrados.