Un grupo de investigadores del Centro CISPA Helmholtz para la Seguridad de la Información en Alemania ha revelado un fallo arquitectónico que afecta a los procesadores RISC-V XuanTie C910 y C920 de la empresa china de chips T-Head. Este fallo podría permitir a los atacantes obtener acceso ilimitado a los dispositivos vulnerables.

La vulnerabilidad ha sido denominada GhostWrite y se describe como un error de CPU directamente integrado en el hardware, a diferencia de un ataque de canal lateral o de ejecución transitoria.

> *«Esta vulnerabilidad permite a atacantes sin privilegios, incluso aquellos con acceso limitado, leer y escribir en cualquier parte de la memoria del equipo y controlar dispositivos periféricos como las tarjetas de red. GhostWrite inutiliza las funciones de seguridad de la CPU y no puede corregirse sin desactivar aproximadamente la mitad de la funcionalidad de la CPU»*, explicaron los investigadores.

CISPA descubrió que la CPU contiene instrucciones defectuosas en su extensión vectorial, un componente adicional del conjunto de instrucciones RISC-V diseñado para manejar datos más grandes que el conjunto de instrucciones básico (ISA).

Estas instrucciones defectuosas, que según los investigadores operan directamente sobre la memoria física en lugar de la memoria virtual, podrían eludir el aislamiento de procesos que normalmente implementan el sistema operativo y el hardware.

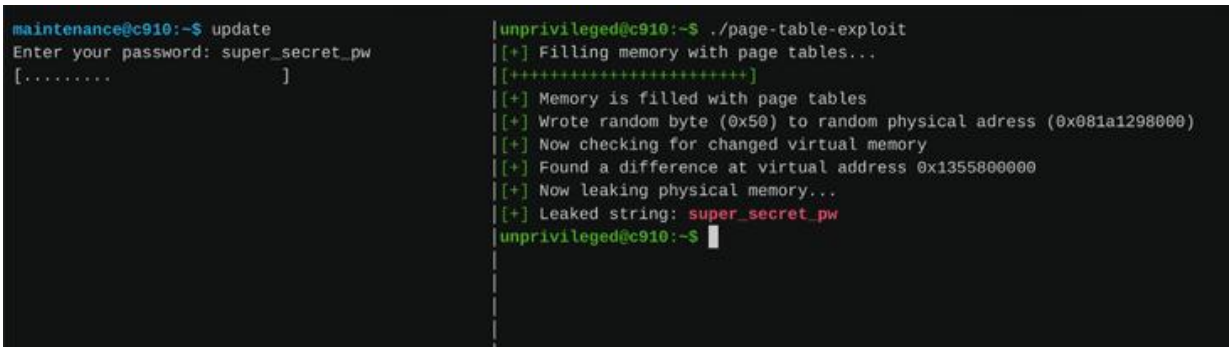
Como resultado, un atacante sin privilegios podría explotar esta vulnerabilidad para escribir en cualquier ubicación de la memoria y evitar las medidas de seguridad y aislamiento, logrando así un acceso completo e irrestricto al dispositivo. También podría filtrar cualquier contenido de la memoria de una máquina, incluidas contraseñas.

> *«El ataque es completamente fiable, determinista y tarda solo microsegundos en ejecutarse. Incluso las medidas de seguridad como la contenedorización en Docker*

> *o el sandboxing no pueden detener este ataque. Además, el atacante puede tomar control de dispositivos de hardware que usan entrada/salida mapeada en memoria (MMIO), permitiéndoles enviar cualquier comando a estos dispositivos»,* indicaron los investigadores.

La contramedida más efectiva contra GhostWrite es desactivar toda la funcionalidad vectorial, lo que, sin embargo, afecta gravemente el rendimiento y las capacidades de la CPU, ya que apaga aproximadamente el 50% del conjunto de instrucciones.

> *«Afortunadamente, las instrucciones vulnerables se encuentran en la extensión vectorial, que puede ser desactivada por el sistema operativo. Esto mitiga por completo GhostWrite, pero también desactiva completamente las instrucciones vectoriales en la CPU»,* señalaron los investigadores.



> *«Desactivar la extensión vectorial reduce significativamente el rendimiento de la CPU, especialmente en tareas que se benefician del procesamiento paralelo y el manejo de grandes conjuntos de datos. Las aplicaciones que dependen en gran medida de estas funciones pueden experimentar una disminución en el rendimiento o una funcionalidad reducida».*

Esta revelación coincide con el anuncio del equipo de seguridad de Android en Google, que ha descubierto más de nueve vulnerabilidades en la GPU Adreno de Qualcomm. Estas vulnerabilidades podrían permitir a un atacante con acceso local a un dispositivo escalar privilegios y ejecutar código a nivel de kernel. El fabricante de los chipsets ha corregido las debilidades.

Además, se ha descubierto una nueva falla de seguridad en los procesadores de AMD que podría ser explotada por un atacante con acceso al kernel (conocido como Ring-0) para elevar privilegios y modificar la configuración del Modo de Gestión del Sistema (SMM o Ring-2) incluso cuando el Bloqueo SMM está habilitado.

Conocida como Sinkclose por IOActive (también identificada como CVE-2023-31315, con una calificación CVSS de 7.5), se informa que la vulnerabilidad ha pasado desapercibida durante casi veinte años. El acceso a los niveles más altos de privilegio en una computadora permite desactivar características de seguridad e instalar malware persistente que puede permanecer prácticamente invisible.

En una conversación con WIRED, la empresa mencionó que la única manera de solucionar una infección sería conectarse físicamente a las CPUs utilizando una herramienta de hardware llamada programador SPI Flash y escanear la memoria en busca de malware instalado a través de SinkClose.

> *«Una validación inadecuada en un registro específico del modelo (MSR) podría permitir que un programa malicioso con acceso a nivel ring0 altere la configuración de SMM mientras el bloqueo de SMI está activado, lo que potencialmente podría resultar en la ejecución de código arbitrario»*, señaló AMD en un comunicado, indicando que planea lanzar actualizaciones a los fabricantes de equipos originales (OEM) para abordar el problema.