Hace un tiempo informamos sobre la vulnerabilidad Row Hammer, un problema crítico que afecta a los chips modernos DRAM (memoria de acceso aleatorio dinámico) que podría permitir a los hackers obtener mayores privilegios de kernel en un sistema objetivo al acceder repetidamente a las celdas de memoria e inducir cambios de bits.

Para mitigar la vulnerabilidad de RowHammer en la última DRAM DDR4, muchos fabricantes de chips de memoria agregaron algunas defensas bajo el término general Target Row Refresh (TRR) que actualiza las filas adyacentes cuando se accede a una fila de la víctima más allá de un umbral.

Sin embargo, Target Row Refresh, promovido como una protección para mitigar los ataques de RoeHammer, también es insuficiente y podría permitir a los atacantes ejecutar nuevos patrones de martilleo y volver a habilitar los ataques de volteo de bits en el último hardware.

TRRespass

Rastreada como CVE-2020-10255, la vulnerabilidad recientemente reportada fue descubierta por investigadores de VUSec Lab, que hoy lanzaron TRRespass, una herramienta de fuzzing RowHammer de caja abierta de muchos lados que puede identificar patrones sofisticados de martilleo para montar en el mundo real de ataques.

La última falla también afecta a los chips LPDDR4 y LPDDR4X integrados en la mayoría de los smartphones modernos, dejando a millones de dispositivos vulnerables a RowHammer nuevamente.

> *«También portamos una versión simplificada de TRRespass a ARM y logramos activar cambios de bits en una variedad de teléfonos inteligentes como Google Pixel 3 y Samsung Galaxy S10»,* dijeron los investigadores.

Target Row Refresh intenta identificar posibles filas de víctimas contanto el número de activaciones de filas adyacentes y comparándolas con un valor predefinido, pero aún es incapaz de mantener la información sobre todas las filas a las que se accede al mismo tiempo para la mitigación eficaz de los cambios de bits por medio de las filas de agresores.

> *«Las variantes conocidas de RowHammer usan como máximo dos filas de agresores para realizar el ataque, un pequeño número de filas a las que se accede con frecuencia puede ser fácilmente monitoreado por TRR. Pero ¿qué pasa si usamos más filas de agresores?»*, agregaron los investigadores.
>
> *«Pero tener más agresores abruma la mitigación de TRR ya que solo puede rastrear algunas filas de agresores a la vez. Los chips DDR4 afortunadamente son más vulnerables, lo que nos da la posibilidad de reducir el número de acceso a cada uno de los agresores para activar cambios de bits, o, en otras palabras, aumentar el número de agresores para evitar la mitigación».*

Los investigadores afirmaron que *«probamos TRREspass en los tres principales proveedores de memoria (comprometiendo más del 99% del mercado) usando 42 DIMM»,* y encontraron pequeños cambios en 12 de ellos.

El equipo de VUSec informó los nuevos ataques de RowHammer a todas las partes afectadas a fines del año pasado, pero, desafortunadamente no será reparado en un tiempo corto.