Expertos en seguridad cibernética de ETH Zurich han ideado una nueva versión del ataque RowHammer a la memoria DRAM (memoria de acceso aleatorio dinámico) que, por primera vez, logra afectar exitosamente a sistemas AMD Zen 2 y Zen 3 a pesar de las contramedidas como el Target Row Refresh (TRR).

> *«Este descubrimiento confirma que los sistemas AMD son tan susceptibles al Rowhammer como los sistemas Intel, lo que amplía considerablemente la superficie de ataque, dado que AMD tiene actualmente una participación de mercado del 36% en las CPUs de escritorio x86»,* afirmaron los investigadores.

Esta técnica ha sido nombrada ZenHammer, y también puede provocar cambios en los bits por RowHammer en dispositivos DDR5 por primera vez.

El ataque RowHammer, divulgado inicialmente en 2014, es un conocido método que explota la arquitectura de celdas de memoria de la DRAM para modificar datos al acceder repetidamente a una fila específica (conocido como «martilleo»), provocando que la carga eléctrica de una celda se filtre a celdas adyacentes.

Esto puede causar cambios aleatorios en los bits de las filas de memoria vecinas (de 0 a 1, o viceversa), lo que altera el contenido de la memoria y potencialmente facilita la escalada de privilegios, comprometiendo la confidencialidad, integridad y disponibilidad de un sistema.

Estos ataques aprovechan la proximidad física de estas celdas dentro de la matriz de memoria, un problema que es probable que empeore a medida que continúe la escala de la tecnología DRAM y aumente la densidad de almacenamiento.

> *«A medida que la tecnología DRAM sigue avanzando, los cambios de bits por RowHammer pueden ocurrir con menos activaciones, lo que significa que las tasas de activación de filas de la DRAM para tareas regulares pueden acercarse o incluso superar el umbral de RowHammer»,* señalaron los investigadores de ETH Zurich en

> un artículo publicado en noviembre de 2022.

«Por lo tanto, un sistema podría experimentar cambios en los bits o activar con frecuencia mecanismos de defensa de RowHammer incluso sin que un actor malintencionado realice un ataque de RowHammer en el sistema, lo que podría resultar en corrupción de datos o una degradación significativa del rendimiento».

Una de las principales contramedidas implementadas por los fabricantes de DRAM contra RowHammer es TRR, que es un término general utilizado para mecanismos que actualizan las filas objetivo que se determinan como frecuentemente accesadas.

La idea es generar más operaciones de actualización de memoria para que las filas afectadas se actualicen antes de que ocurran cambios de bits o se corrijan después de que ocurran debido a ataques de RowHammer.

ZenHammer, al igual que TRRespass y SMASH, elude las protecciones de TRR al realizar ingeniería inversa de las funciones secretas de direcciones de DRAM en sistemas AMD y adoptar una sincronización de actualización mejorada y programación de instrucciones de eliminación y vallado para provocar cambios de bits en siete de cada 10 dispositivos de muestra Zen 2 y seis de cada 10 dispositivos Zen 3.

El estudio también identificó una secuencia óptima de instrucciones para maximizar las tasas de activación de filas y, por ende, hacer más efectivo el ataque.

> *«Nuestros resultados demostraron que las cargas regulares (MOV) con CLFLUSHOPT para eliminar agresores de la caché, emitidas inmediatamente después de acceder a un agresor (estilo 'disperso'), son las más eficientes»*, indicaron los investigadores.

ZenHammer es el primer método que puede desencadenar cambios de bits en sistemas

equipados con chips DDR5 en la plataforma microarquitectónica Zen 4 de AMD. Sin embargo, solo funciona en uno de los 10 dispositivos probados (Ryzen 7 7700X).

Es importante destacar que los módulos de DDR5 DRAM se consideraban previamente protegidos contra los ataques de RowHammer debido a la sustitución de TRR por un nuevo tipo de protección denominado gestión de actualizaciones.

> *«Los cambios en DDR5, como las mejoras en las mitigaciones de RowHammer, la incorporación de códigos de corrección de errores (ECC) en el propio chip y una frecuencia de actualización más alta (32 ms), dificultan más la ocurrencia de cambios de bits»,* señalaron los investigadores.
>
> *«Dado que no se han detectado cambios de bits en nueve de cada diez dispositivos DDR5, se requiere un trabajo adicional para comprender mejor las posibles nuevas mitigaciones de RowHammer y sus garantías de seguridad».*

AMD, en un comunicado de seguridad, indicó que está evaluando los cambios de bits por RowHammer en dispositivos DDR5 y que proporcionará una actualización una vez que finalice la evaluación.

> *«Los productos microprocesadores de AMD incorporan controladores de memoria diseñados para cumplir con las especificaciones DDR estándar de la industria. La vulnerabilidad a los ataques de RowHammer varía según el dispositivo DRAM, el fabricante, la tecnología y la configuración del sistema»,* añadió.