Rowhammer, La Vulnerabilidad Que Afecta La DRAM

Los investigadores de seguridad intenta averiguar maneras de secuestrar los computadores compatibles con Intel que ejecutan Linux, para aprovecharse de las debilidades físicas en ciertas variedades de DDR DRAM (doble velocidad de datos de memoria dinámica de acceso aleatorio), las cuales se usan para obtener privilegios del núcleo Linux.

La técnica, conocida como «**rowhammer**«, se esbozó en un blog publicado el lunes por iniciativa de seguridad de Google Project Zero, un equipo de los mejores investigadores de seguridad identifica con dedicación vulnerabilidades graves de día cero en diferentes programas. **Rowhammer** es un problema con los chips de DRAM de generación mas reciente, en los que el acceso a varias una fila de memoria varias veces, puede causar «bit flipping» en una fila adyacente, la cual podría permitir a cualquier persona cambiar el valor de los contenidos almacenados en la memoria del ordenador.

¿De Qué Trata El Error Rowhammer?

La **memoria DDR** está formada en una serie de filas y columnas, que se asignan a los distintos servicios, aplicaciones y recursos del sistema operativo en grandes bloques. Con el fin de evitar que cada aplicación acceda a la memoria de otra aplicación, se mantienen en una capa de protección, conocidad como «**Sandbox**«.

Sin embargo, la **protección Sandbox** puede evitarse utilizando la técnica de **bit flipping,** en el que una aplicación maliciosa necesita para acceder repetidamente filas adyacentes de la memoria en una pequeña fracción de segundo.

> *«Con suficientes accesos, este puede cambiar el valor de una celda de 1 a 0, o viceversa. En otras palabras, el área seleccionada cero será transferido a las víctimas, o viceversa. » Explicaron los investigadores.*

La **técnica de bit flipping** se presentó por primera vez en un documento de estudio experimental publicado por la Universidad Carnegie Mellon, titulado, «Flipping Bits in Memory Without Accessing Them: An Experimental Study of DRAM Disturbance Errors.»

Dos Exploits Que Muestran La Vulnerabilidad

Como sabemos, la fabricación de DRAM disminuye la escala características de chips a dimensiones físicas más pequeñas. La última tecnología exige más capacidad de memoria en un chip, por lo que se ha convertido en más difícil de evitar que las células de DRAM interactuen eléctricamente entre sí.

El equipo del Project Zero ha convertido el **bit flipping en un ataque real,** demostrando por dos exploits de prueba de concepto para afrontar con éxito el control de muchos equipos que ejecutan Linux x86 y cree que el mismo podría hacerse con otros sistemas operativos.

- En primer lugar, las entradas de tablas de paginación (PTEs), explotables con rowhammer, pueden ser atacadas con bit flipping para lograr privilegios de kernel en Linux x86 y 64, por tanto, a tener acceso de lectura y escritura a la totalidad de la memoria física.
- Segundo, la explotacion de la vulnerabilidad misma por escapar de la zona de pruebas de Native Client.

Técnicas De Mitigación

Los expertos en seguridad informática, también proporcionaron una forma de mitigar el ataque de privilegio de kernel. Los investigadores cambiaron Native Client para no permitir la **instrucción CLFLUSH x86** que se requiere para hacer el primer exploit.

Con la ayuda de los anteriores exploits, el equipo del Project Zero realizó pruebas en ocho modelos de ordenadores portátiles x86, construidos entre 2010 y 2014, usando cinco diferentes proveedores de DRAM DDR3 y cinco familias de CPU diferentes. Un gran subconjunto de estas máquinas, es decir, 15 de los 29 resultaron ser vulnerables.