Un equipo de investigadores de seguridad cibernética reveló ayer los detalles de un nuevo ataque de canal lateral a la memoria dinámica de acceso aleatorio (DRAM), que permitiría a los programas maliciosos instalados en un sistema reciente leer datos confidenciales de la memoria de otros procesos que se ejecutan en el mismo hardware.

RAMBleed es el nombre que se le dio a la vulnerabilidad CVE-2019-0174, el ataque se basa en una conocida clase de ataque de canal lateral DRAM llamado Rowhammer, de la que existen algunas varianes como GLitch, RAMpage, Throwhammer, Nethammer, Drammer, etc.

Conocido desde 2012, el error Rowhammer es un problema de confiabilidad del hardware que se encontró en la nueva generación de chips DRAM.

El acceso repetido y rápido (hammering) a una fila de la memoria puede causar cambios de bit en las filas adyacentes, lo que significa que cambia sus valores de bit de 0 a 1 y viceversa.

En los siguientes años, los investigadores también demostraron explotaciones exitosas para lograr una escalada de privilegios en las computadoras vulnerables al voltear bits en la memoria de la víctima.

Descubierto por un equipo de investigadores de la Universidad de Michigan, la Universidad Tecnológica de Graz y la Universidad de Adelaida, el nuevo RAMBleed también se basa en el mecanismo de giro de bits, pero en lugar de escribir datos en las filas adyacentes, este ataque permite a los hackers leer la información en la memoria protegida que pertenece a otros programas y usuarios.

> *«Más específicamente, mostramos cómo un atacante sin privilegios puede explotar la dependencia de los datos entre los cambios de bits inducidos por Rowhammer y los bits en las filas cercanas para deducir estos bits, incluidos los valores que pertenecen a otros procesos y al núcleo. Por lo tanto, la contribución principal de este trabajo es demostrar que Rowhammer es una amenaza no solo para la*

> *integridad sino también para la confidencialidad»,* dijeron los investigadores.

En la imagen se observa que si un atacante quiere leer datos secretos contenidos en las celdas de memoria «*secretas*», tiene que:

- Encontrar una página de muestreo, en el mismo desplazamiento en una página de memoria que el bit secreto.
- Manipular el diseño de la memoria utilizando técnicas de mensaje de memoria para colocar cuidadosamente los datos secretos de la víctima en las filas que están arriba y debajo de la fila de la memoria del atacante, de modo que el bit que se invierte en las filas del atacante se vuelva dependiente de los valores de la memoria.
- Martillar las filas A0 y A2 e inducir cambios de bit en la fila A1 (página de muestreo), cuyo valor inicial se estableció en 1, lo que influye en su valor utilizando los datos de la víctima en celdas «secretas».

> *«Si el bit se invirtió, el atacante deduce que el valor del bit secreto es 0. De lo contrario, el atacante deduce que el valor es 1. La repetición del procedimiento con bits intercambiables en diferentes desplazamientos en la página permite al atacante recuperar todos los bits secretos de la víctima»*, explicaron los investigadores.

Para demostrar la técnica del canal lateral de lectura, los investigadores presentaron un ataque contra OpenSSH 7.9 que se ejecuta en una máquina Linux y extrajeron con éxito una clave RSA-2048 del demonio SSH de nivel raíz.

Según los investigadores, incluso las protecciones de memoria ECC, que pueden detectar y corregir los cambios de bits no deseados y también mitigan muchos ataques basados en Rowhammer, no evitan el ataque RAMBleed.

Aunque tanto DDR3 como DDR4 son vulnerables a los ataques RAMBleed, los investigadores aconsejaron a los usuarios mitigar el riesgo al actualizar su memoria a DDR4 con la actualización de fila dirigida (TRR) habilitada, ya que es más difícil de explotar.