En los últimos años, algunos grupos de investigadores de ciberseguridad han revelado decenas de vulnerabilidades de canal lateral de memoria en procesadores modernos y DRAM, como Rowhammer, RAMBleed, Spectre y Meltdown.

Todas estas vulnerabilidades tienen una particularidad en común, OpenSSH. Como una prueba de concepto, muchos investigadores demostraron sus ataques de canal lateral contra la aplicación OpenSSH instalada en una computadora específica, donde un proceso sin privilegios propiedad de un atacante, explota las vulnerabilidades de lectura de la memoria para robar claves privadas SSH secretas de las regiones de memoria restringida del sistema.

Eso es posible porque OpenSSH tiene un agente que mantiene una copia de su clave SSH en la memoria para que no tenga que escribir su frase de contraseña cada vez que quiera conectarse al mismo servidor remoto.

Sin embargo, los sistemas operativos modernos almacenan de forma predeterminada los datos confidenciales, incluidas las claves de cifrado y las contraseñas, en la memoria del núcleo, a la que no se puede acceder mediante procesos privilegiados de nivel de usuario.

Pero como dichas claves SSH viven en la memoria RAM o CPU en formato de texto simple, la función es susceptible de intentos de piratería cuando los ataques involucran vulnerabilidades de lectura de memoria.

OpenSSH ahora solo almacena claves cifradas en la memoria

La última actualización de los desarrolladores de OpenSSH resuelve este problema mediante la introducción de una nueva función de seguridad que encripta las claves privadas antes de almacenarlas en la memoria del sistema, protegiéndola de casi todos los tipos de ataques de canal lateral.

Según el desarrollador de OpenSSH, Damien Miller, un nuevo parche para OpenSSH ahora *«encripta las claves privadas cuando no están en uso con una clave simétrica que se deriva de una 'prekey', relativamente grande que consiste en datos aleatorios (actualmente 16*

KB)».

> *«Los atacantes deben recuperar toda la prekey con gran precisión antes de que puedan intentar descifrar la clave privada protegida, pero la generación actual de ataques tiene tasas de error de bits que, cuando se aplican de forma acumulativa a toda la prekey, hacen esto poco probable»*, dijo Miller.
>
> *«En cuanto a la implementación, las claves se cifran 'protegidas' cuando se cargan y luego se desprenden de forma transparente y automática cuando se usan para firmas o cuando se guardan/serializan»,* agregó.

Cabe mencionar que este parche solo mitiga la amenaza y no es una solución permanente. Miller asegura que OpenSSH eliminará esta protección contra ataques de canal lateral en pocos años cuando la arquitectura de la computadora sea menos insegura.