Una nueva variante de la vulnerabilidad de canal lateral Spectre (Variante 1) ha sido descubierta. Afecta a todas las CPU Intel modernas, y probablemente también a algunos procesadores AMD, que aprovechan la ejecución especulativa para un alto rendimiento, según advirtieron Microsoft y RedHat.

Identificada como CVE-2019-1125, la vulnerabilidad podría permitir a los hackers locales no privilegiados acceder a la información confidencial almacenada en la memoria del kernel privilegiado del sistema operativo, incluyendo contraseñas, tokens y claves de cifrado, que de otro modo serían inaccesibles.

La ejecución especulativa es un componente central del diseño moderno de microprocesador que ejecuta instrucciones especulativas basadas en suposiciones que se consideran verdaderas. Si los supuestos resultan válidos, la ejecución sigue, de lo contrario se descarta.

Dichas ejecuciones especulativas también cuentan con efectos secundarios que no se restauran cuando se desenrolla el estado de la CPU, lo que lleva a la divulgación de información, a la que luego se puede acceder mediante ataques de canal lateral.

Microsoft emitió de forma silenciosa parches para la nueva vulnerabilidad de ejecución especulativa en su actualización de seguridad del martes para julio de 2019, que fue descubierta y revelada de forma responsable por investigadores de seguridad de Bitdefender.

Según un aviso de seguridad publicado ayer por Red Hat, el ataque se basa en la ejecución especulativa de instrucciones SWAPGS inesperadas luego de que una sucursal se pronostica de forma errónea.

La instrucción SWAPGS es una instrucción de sistema privilegiada que intercambia los valores en el registro GS con los valores MSR y solo está disponible en dispositivos con arquitectura X86-64.

> *«Esto se logra al abusar del hecho de que la instrucción SWAPGS se puede ejecutar de forma especulativa. Un atacante puede forzar desreferencias arbitrarias de memoria en el núcleo, lo que deja rastros dentro de los cachés de datos. El atacante puede recoger estas señales para inferir el valor ubicado en la dirección del núcleo dada»,* dicen los investigadores de Bitdefender.

El ataque SWAPGS rompe el aislamiento de la tabla de páginas del núcleo (KPTI) proporcionado por las CPU modernas y se puede utilizar para filtrar la memoria del núcleo sensible del modo de usuario no privilegiado, aseguró Intel.

> *«Es posible que estas ramas condicionales en el código de entrada del kernel de Linux puedan especular erróneamente en un código que no realizará los SWAPGS, lo que da como resultado una ventana de ejecución especulativa durante la cual se utiliza el GS incorrecto para operaciones de memoria independientes»,* dijo Red Hat.

Según los investigadores de Bitdefender, el nuevo ataque evita todas las mitigaciones conocidas implementadas luego del descubrimiento de las vulnerabilidades Spectre y Meltdown a inicios de 2018, que ponen en riesgo a prácticamente todas las computadoras del mundo.

Aunque el kernel de Linux también contiene un dispositivo que puede explotarse para atacar sistemas Linux, los investigadores creen que explotar los sistemas operativos Linux podría ser un poco más difícil que las computadoras con Windows.

Ya que el ataque no puede iniciarse de forma remota, es poco probable que cause infecciones masivas de malware, como EternalBlue se usó para WannaCry, pero, puede explotarse como parte de un ataque extremadamente dirigido.

Los usuarios afectados pueden abordar el problema por medio de una actualización de software para sus sistemas operativos que mitigaría cómo la CPU accede de forma

especulativa a la memoria.

Mientras tanto, Google también preparó un parche para corregir esta vulnerabilidad en su ChromeOS 4.19, con una actualización que se lanzará próximamente, describiendo la falla como:

> *«Un atacante puede entrenar al predictor de rama para saltear especulativamente la ruta de swapgs para una interrupción o excepción. Si inicializan el registro GS a un valor de espacio de usuario, si los swapgs se saltan especulativamente, los accesos de percpu relacionados con GS posteriores en la ventana de especulación se realizarán con el valor GS controlado por el atacante. Esto podría provocar que se acceda y se filtre la memoria privilegiada».*

Por otro lado, AMD dijo:

> *«Según el análisis externo e interno, AMD cree que no es vulnerable a los ataques de la variante SWAPGS porque los productos AMD están diseñados para no especular sobre el nuevo valor GS luego de un SWAPGS especulativo. Para el ataque no es una variante SWAPGS, la mitigación es para implementar nuestras recomendaciones existentes para la variante 1 de Spectre».*