Los procesadores modernos Intel y AMD son susceptibles a una nueva forma de ataque de canal lateral que hace que los ataques de memoria caché basados en vaciado sean resistentes al ruido del sistema, según una investigación recientemente publicada.

Los hallazgos publicados en el artículo *«DABANGG: Time for Fearless Flush based Cache Attacks»,* publicados por los investigadores Biswabandan Panda y Anish Saxena, del Instituto Indio de Tecnología (IIT) Kunpur, a inicios de la semana pasada.

Apodado *«Dabangg»* (Intrépido), el enfoque se basa en los ataques Flush + Reload y Flush + Flush, que han sido explotados previamente por otros investigadores para filtrar datos de las CPU de Intel.

Sin embargo, la nueva variante tiene como objetivo mejorar la precisión de los ataques incluso en un sistema multinúcleo. También funciona a la perfección contra sistemas operativos que no son Linux, como macOS.

> *«Al igual que cualquier otro ataque de caché, los ataques de caché basados en vaciado dependen de la calibración de la latencia de caché. Los ataques de sincronización de caché de última generación no son efectivos en el mundo real ya que la mayoría de ellos trabajan en un entorno altamente controlado»,* dijo Biswabandan, profesor asistente en IIT Kanpur.
>
> *«Con DABANGG, hacemos un caso para los ataques de caché que pueden tener éxito en el mundo real que es resistente al ruido del sistema y funciona perfectamente incluso en un entorno altamente ruidoso»,* agregó.

Los ataques Flush+Reload y Flush+Flush funcionan mediante el vaciado de la línea de memoria (con la instrucción *«clflush»*), luego esperando que el proceso de la víctima acceda a la línea de memoria y posteriormente recargando (o vaciando) la línea de memoria, midiendo el tiempo necesario para cargarlo.

DABANGG es similar a los ataques Flush+Reload y Flush+Flush en el sentido de que es un ataque basado en color, que depende de la diferencia de tiempo de ejecución entre los accesos de memoria en caché y no en caché. Pero a diferencia de los dos últimos, DABANGG hace que los umbrales utilizados para diferenciar un hit de caché de una dinámica de fallas.

Las técnicas de administración de energía como escala dinámica de voltaje y frecuencia (DVFS) en los procesadores modernos, permiten cambios de frecuencia basados en la utilización general de la CPU, con núcleos que ejecutan procesos intensivos en cómputo que funcionan a una frecuecia más alta que los que no lo hacen.

Esta diferencia de frecuencia en el núcleo resulta en una latencia de ejecución variable para las instrucciones, y hace que los umbrales elegidos para distinguir un acierto de caché de una falla sean inútiles, según los investigadores.

> *«Hacemos que estos umbrales sean dinámicos en función de la frecuencia del procesador (que se acelera hacia arriba y hacia abajo según los controladores DVFS), lo que a su vez hace que los ataques basados en el flujo sean resistentes al ruido del sistema»,* dijo el profesor Panda.

DABANGG refina las deficiencias al capturar la distribución de frecuencia del procesador en la etapa previa al ataque y utilizando un código de cálculo pesado para estabilizar la frecuencia, antes de proceder con un ataque Flush+Reload o Flush+Flush para calcular la latencia y verificar un golpe de caché.

Debido a que DABANGG también es un ataque basado en color, puede mitigarse utilizando las mismas técnicas correspondientes a Flush+Reload y Flush+Flush, es decir, modificando la instrucción clflush y monitoreando las fallas de caché, además de realizar cambios de hardware para prevenir los ataques.

> *«Los ataques basados en la descarga deben ser conscientes de la frecuencia del*

> *procesador para una mejor precisión. En términos generales, si un ataque no puede atacar efectivamente el acceso de una víctima a menos que se controlen todas las condiciones, ese ataque no representa un riesgo en el mundo real. Creemos que esto es solo el comienzo en términos de empujar los ataques de caché al mundo real, y desencadenará ataques de caché mejores y más robustos en el futuro»,* dijo Panda.

Los investigadores lanzarán el código fuente de la prueba de concepto en GitHub después del 15 de junio de 2020.