




Meltdown y Spectre

Sistemas
Operativos
2020-2

Medina Molina Fernando Arturo
Osorio Robles Sergio

Introducción

En la actualidad, la información existente dentro de nuestros dispositivos llega a ser de suma importancia, ya que no solamente le confiamos información empresarial, sino que también tenemos información personal, desde cuentas bancarias, estados de cuenta, salud, etc. y todo ello es representado en bits y bytes que son almacenados en los mismos con diversas finalidades. Es por ello que en las empresas toda ésta información es objeto de gran valor, teniendo como prioridad la seguridad informática afectando gobiernos, institutos, empresas e individuos. En esta presentación hablaremos de un par que ha tomado gran relevancia actualmente. [Meltdown](#) y [Spectre](#)



Meltdown

Como hablamos, es una vulnerabilidad o “agujero de seguridad” por hardware afectando principalmente a los procesadores x86, IBM POWER y algunos ARM, básicamente consiste en romper el aislamiento entre el usuario y el Sistema Operativo, permitiendo el acceso a memoria sin autorización, accediendo a los datos tanto del sistema, como a los de programas sean privados o no. Siendo un aspecto importante que no solamente puede filtrarse información desde una computadora personal, sino que también en la nube. Fue encontrado en enero de 2018 asignado con el identificador CVE-2017-5754.





También es conocido como carga maligna de la caché de datos (Rogue Data Cache Load). Explota una condición de carrera inherente al diseño de muchas CPU actuales. Esta condición se da entre los accesos a la memoria y la comprobación de privilegios durante el procesamiento de instrucciones. Además, en combinación con un ataque de canal lateral a la caché de la CPU, esta vulnerabilidad permite que un proceso se salte las comprobaciones habituales de nivel de privilegio que normalmente aislarían al proceso maligno e impedirían que accediese a datos que pertenecen al sistema operativo y otros procesos concurrentes.

Pasos

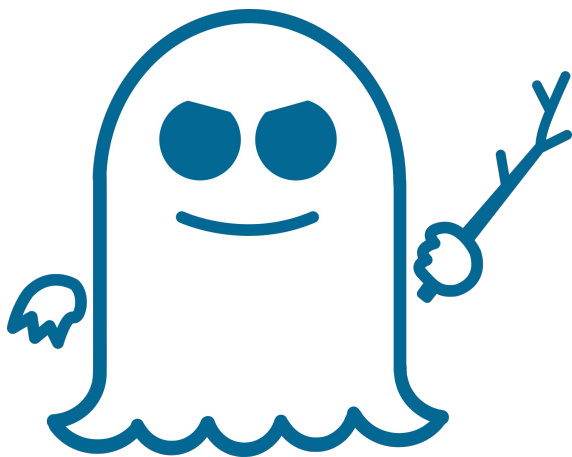
Paso 1: El contenido de una ubicación de memoria elegida por el atacante se carga a la acción, que es inaccesible para el atacante en un registro.

Paso 2: Una instrucción transitoria accede a una línea de caché basado en el contenido secreto del registro.

Paso 3: El atacante usa Flush + Reload para determinar si accedió a la línea de caché y, por lo tanto, el secreto almacenado en la ubicación de memoria elegida



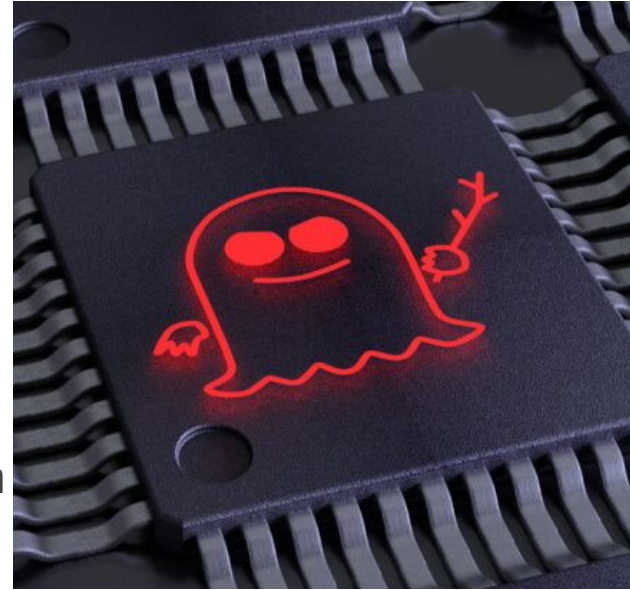
Spectre



Es una vulnerabilidad que afecta a los microprocesadores modernos que utilizan predicción de saltos. En la mayoría de los procesadores, la ejecución especulativa que surge de un fallo de la predicción puede dejar efectos observables colaterales que pueden revelar información privada a un atacante. Se han emitido dos ID de Vulnerabilidades y Exposiciones Comunes (siglas en inglés CVE) relacionados con Spectre, CVE-2017-5753 (variante 1, baipás de la comprobación de límites) y CVE-2017-5715 (variante 2, inyección de destino del salto).

Se ha descubierto que los motores JIT empleados para JavaScript son vulnerables. Un sitio web podría leer información guardada en el navegador que pertenece a otro sitio web, o acceder a información alojada en la memoria que está utilizando el navegador.

Los ataques de espectro implican inducir a una víctima a especular realizar operaciones que no ocurrirían durante el programa correcto ejecución y que filtran la información confidencial de la víctima a través de un canal lateral al adversario.




Pasos

Primero, muestra que la lógica de la predicción de saltos de los procesadores actuales puede ser entrenada para acertar o fallar en sus pronósticos.

En segundo lugar, muestra que las diferencias subsiguientes entre los aciertos y los fallos de la caché pueden medirse de forma fiable.

En tercer lugar, el documento sintetiza los resultados obtenidos con trucos de la programación orientada a retorno.

Por último, el documento concluye generalizando el ataque a cualquier estado no funcional del proceso tomado como víctima.





DEMOSTRACIÓN



Referencias

- Moritz Lipp, Michael Schwarz,et. Al. (2018). Meltdown: Reading Kernel Memory from User Space. 16/2/2020, de Graz University of Technology,Cyberus Technology GmbH,et. al Sitio web: <https://meltdownattack.com/meltdown.pdf>
- Paul Kocher, Jann Horn,et. al. (2018). Spectre Attacks: Exploiting Speculative Execution. 16/2/2020, de Google Project Zero, G DATA Advanced Analytics, 4 University of Pennsylvania and University of Maryland, et. al Sitio web: <https://meltdownattack.com/meltdown.pdf>
- Meltdown(vulnerabilidad).(Sin fecha).En Wikipedia. Recuperado el 2/3/2020 de: [https://es.wikipedia.org/wiki/Meltdown_\(vulnerabilidad\)](https://es.wikipedia.org/wiki/Meltdown_(vulnerabilidad)).