Sistemas Operativos I

Problemática: Problemas de seguridad en el procesador

Alumno: Vicente Mata Velasco

Profesor: Eduardo Flores Gallegos

Fecha: 09/05/2018

Identificado un grave problema de seguridad en los procesadores Intel

Un grave fallo de diseño en los procesadores Intel fabricados en la última década afecta a la seguridad de los equipos que gobiernan. Según este medio, este error permitiría que los hackers o cualquier otro programa tuvieran acceso al kernel, el conocido corazón del sistema en el que se almacenan datos sensibles del usuario, como las contraseñas y coordenadas de acceso a cuentas. Se trata de un problema de gran impacto entre los usuarios, dada la gran presencia del fabricante en el mercado. La solución obliga a parchear los equipos, lo que puede ralentizarlos.

El fabricante ha sido contundente al calificar como "imprecisas" las acusaciones vertidas, y ha explicado que está trabajando con otras marcas del mercado para proporcionar una solución global al exploit. El gigante ha comenzado ya a trabajar, dice, con las plataformas para distribuir parches que solucionarían el problema, y contrariamente a lo que inicialmente se había sugerido, esta solución no ralentizará en absoluto los sistemas, asegura.

(ZURIARRAIN, 2018)

Orígenes del problema

Aunque la información está bajo embargo por cuestiones de seguridad y por lo tanto podemos dar todos los detalles se ha identificado un grave problema de seguridad en el diseño de los procesadores Intel lanzados durante los últimos diez años, lo que quiere decir que está presente desde el lanzamiento de los procesadores Core de primera generación hasta los actuales de octava generación.

Echando un vistazo a la información que hemos podido ver parece que ese error se produce en el sistema que establece el control entre el Kernel de cada sistema operativo, los permisos de acceso y el procesador.

(Ros, 3)

En que consiste el problema

El Kernel (núcleo) de cada sistema operativo dispone de varios subniveles en los que se guardan diferentes datos de gran importancia, que pueden ir desde los procesos hasta los registros y las contraseñas. Esos subniveles se controlan mediante permisos determinados que se atribuyen para permitir el acceso a unos y otros, y es ahí donde está el problema.

El error hace que no se pueda controlar de la manera apropiada la concesión de esos permisos de acceso, lo que en teoría permitiría a un atacante acceder a sectores restringidos del Kernel a pesar

de no contar con los permisos necesarios para ello y hacerse con toda la información que encuentre en ellos.

Como anticipamos es una cuestión grave, ya que permitiría un acceso total al Kernel obviando la obtención de permisos. Por otro lado hay que tener en cuenta que se trata de un error presente a nivel de hardware, lo que significa que Intel no puede resolverlo mediante una simple actualización de microcódigo y que por tanto no tiene una solución fácil de implementar.

Al ser un fallo importante que está extendido a generaciones de procesadores lanzados durante los últimos diez años la solución más “simple” está en que los principales sistemas operativos se actualicen para resolver este problema, y esto incluye tanto a Windows como a Linux y a MacOS.

(Ros, 3)

Meltdown y Spectre

Investigadores de Google Project Zero y del Instituto de Procesamiento de Información Aplicada y Comunicaciones (IAIK) en la Universidad Tecnológica de Graz (TU Graz) han descubierto varias vulnerabilidades que afectan a procesadores que se incluyen en multitud de dispositivos como portátiles, tablets, smartphones entre otros. Las vulnerabilidades forman parte de una característica de la arquitectura integrada en los microprocesadores que en principio se usa para mejorar el rendimiento del sistema conocido como ejecución especulativa.

Existen dos tipos de ataques para explotar las vulnerabilidades: el bautizado como “Meltdown” que podría permitir acceder a la memoria del sistema operativo principalmente; y “Spectre”, que facilita el acceso a la memoria entre aplicaciones. Esto significaría, por ejemplo, que si un malware es programado para acceder a la memoria aprovechando esta vulnerabilidad, podría conocer toda la información que en ella se almacena, desde contraseñas hasta los datos de un monedero de criptomonedas.

(Desconocido, 2018)

- **Meltdown:** Como revela ese estudio, este ataque permite a un programa acceder a la memoria (y secretos) de otros programas y del sistema operativo. "Meltdown rompe el aislamiento fundamental que existe entre las aplicaciones de usuario y el sistema operativo". El problema afecta a ordenadores personales y a la infraestructura cloud (es el problema del que hablábamos ayer y que afecta, que se sepa, a procesadores de Intel). Es importante destacar que hay parches software para atajar los ataques Meltdown.
- **Spectre:** Este problema va más allá y "rompe el aislamiento entre distintas aplicaciones". Un atacante podría usarlo para vulnerar la seguridad de aplicaciones que han sido programadas perfectamente y "siguiendo las mejores prácticas", y de hecho seguir esas

> prácticas acaba siendo irónicamente contraproducente, ya que hace estos programas más vulnerables a Spectre. A diferencia de Meltdown, no hay parches software para Spectre, que eso sí, es más difícil de explotar que Meltdown, pero también "más difícil de mitigar". Algunos parches software pueden evitar ataques Spectre con exploits conocidos que traten de aprovechar esta vulnerabilidad.

Meltdown afecta a todos los procesadores Intel que hagan uso de la tradicional Out-of-Order Execution, y eso incluye básicamente a todos los que están funcionando a día de hoy en nuestros equipos, ya que estos procesadores llevan produciéndose desde 1995. Solo los Itanium y los Intel Atom desarrollados antes de 2013 están fuera de peligro. Los investigadores no han podido comprobar de momento si el problema afecta también a los procesadores de ARM y de AMD, y solo indican que "no está claro" si también podrían estar expuestos.

(Pedroza, 2018)

Acciones

En la actualidad no existe una solución universal que permita resolver el problema por lo que cada fabricante deberá implementar un parche que permita corregir el fallo.

Algunos fabricantes ya disponen de actualizaciones para solucionar esta vulnerabilidad (ver el apartado de referencias).

En un comunicado, Intel afirmó estar trabajando muy de cerca con otras compañías tecnológicas, tanto fabricantes de procesadores como los creadores de sistemas operativos, para desarrollar una solución de industria que resuelva esta afectación rápida y constructivamente. De hecho, tanto Windows como Linux ya han lanzado actualizaciones para solucionar la brecha de seguridad.

(Berengueras, 2018)

Parches

Las diversas empresas tecnológicas ya se han pronunciado y como comentábamos, los parches que tratan de dar solución a estos problemas o que tratan al menos de mitigarlos están en pleno desarrollo. Los desarrolladores del kernel Linux fueron los primeros en plantear los llamados parches KAISER, y hay ya nuevas versiones del kernel con esos parches aplicados que irán llegando a las distintas distribuciones Linux a través de los gestores de paquetes.

Microsoft por su parte ha publicado un parche de emergencia para todos los dispositivos basados en Windows 10, pero habrá más actualizaciones pronto. En Apple, que se ha mantenido al margen del debate por el momento, sí han publicado un parche parcial con la versión 10.13.2 de macOS.

Los investigadores de Google daban muchos más detalles técnicos sobre el funcionamiento de estos ataques en el blog oficial de Project Zero, y allí explicaban cómo el problema afecta tanto a

dispositivos Android y Chrome OS, aunque según esos expertos explotar la vulnerabilidad "es difícil y limitado en la mayoría de dispositivos Android".

El blog de seguridad de Google tienen más información al respecto, y en él se puede comprobar qué acciones hay que realizar en distintas plataformas de Google (Android, Google Apps, Google Chrome/OS) o productos que como los Chromecast o Google Home no están afectados por el problema.

En el ámbito de la infraestructura cloud, donde los riesgos son igualmente enormes (imprevisibles, pero aparentemente son incluso más preocupantes) las empresas también están actuando, como decíamos ayer. En Azure han decidido adelantar sus mantenimientos programados, que se efectuarán durante esta madrugada (3:30 PM PST, 3 de enero de 2018). Amazon también ha publicado un comunicado en el que avisa de que la mayoría de las instancias de Amazon EC2 están protegidas (suponemos que hablan de Meltdown) y habrá más actualizaciones en el futuro.

(Pedroza, 2018)

Riesgo en rendimiento

Los investigadores que han descubierto el caso han avisado que, además, los parches que se lancen pueden tener afectación sobre el rendimiento de los dispositivos, en el caso de Intel, perder hasta un 30% de su potencia. Intel afirma que contrariamente a lo publicado, «para el usuario medio de un ordenador, no deberían ser significante.

(Berengueras, 2018)

El impacto final tras aplicar esos parches y actualizaciones es imprevisible: en Intel indicaban que ese impacto será probablemente despreciable y dependerá de la carga de trabajo, pero otros estudios preliminares a los que aludíamos en nuestros artículos de ayer apuntaban a bajadas de rendimiento de entre el 5 y el 30%. Las incógnitas en este ámbito también son notables, y habrá que esperar a tener más datos para poder confirmar ese impacto en el rendimiento, si es que realmente existe.

(Pedroza, 2018)

Propuesta de solución

Algunos fabricantes ya disponen de actualizaciones para solucionar esta vulnerabilidad.

Para su correcto funcionamiento, se debe actualizar los antivirus previamente a la instalación del parche.

Bibliografía

Berengueras, J. M. (04 de Enero de 2018). *El Periodico*. Recuperado el 9 de Mayo de 2018, de https://www.elperiodico.com/es/tecnologia/20180104/fallo-seguridad-procesadores-intel-como-afecta-6531825

Desconocido. (04 de Enero de 2018). *Oficina de seguridad del iternauta*. Recuperado el 09 de Mayo de 2018, de https://www.osi.es/es/actualidad/avisos/2018/01/problemas-de-seguridad-en-los-procesadores-de-varios-fabricantes

Pedroza, J. (09 de Enero de 2018). *Xataca*. Recuperado el 9 de Mayo de 2018

Ros, I. (2018 de Enero de 3). *MyComputer*. Recuperado el 9 de Mayo de 2018, de https://www.muycomputer.com/2018/01/03/procesadores-intel-problema-seguridad/

ZURIARRAIN, J. M. (4 de Enero de 2018). *El Pais*. Recuperado el 9 de Mayo de 2018, de https://elpais.com/tecnologia/2018/01/03/actualidad/1514995740_506369.html