proactive
Information security.

Ayudamos a Proteger sus Activos de Información

ProActive News Vol.6

Enero 2018

Meltdown & Spectre

Los primeros días del 2018 nos ha sorprendido con una noticia de Seguridad que se destaca sobre las demás. Se han descubierto vulnerabilidades a nivel de procesador y que fueron bautizados por sus descubridores como **Meltdown** y **Spectre** respectivamente, y como es habitual por estos tiempos, cada uno con su logo correspondiente.

De estos problemas, el primero afecta a procesadores de la compañía Intel y el segundo, además de Intel, a procesadores AMD y los de tecnología ARM (que son utilizados en smartphones y tablets).

Resumiendo y sacando de lado las definiciones puramente técnicas, estas vulnerabilidades permiten que procesos que se ejecutan de forma aislada puedan saltarse esa protección y fisgonear los datos de otros procesos que se ejecutan en la misma plataforma, es decir acceder a espacios de memoria del sistema y sus aplicaciones.

Por de pronto, la vulnerabilidad Meltdown, que es más fácil de explotar, ya los fabricantes empezaron a publicar parches de actualización para los diferentes sistemas y plataformas.

Spectre por su parte, es más difícil en términos técnicos, de explotar y también más difícil de solucionar que con solo aplicar parches, según los expertos.

Se recomienda, como toda actualización, tener especial cuidado en la aplicación de parches en sistemas de producción o alto

rendimiento, pues ya se reportaron casos en que los sistemas se volvieron "más lentos" después de aplicar la actualización para el caso específico de Meltdown.

Estas vulnerabilidades tienen los siguientes CVEs (Common Vulnerabilities and Exposures) asignados:

Número CVE	Descripción
CVE-2017-5715	Branch Target Injection, explotado por Spectre
CVE-2017-5753	Bounds Check Bypass, explotado por Spectre
CVE-2017-5754	Rogue Data Cache Load, explotado por Meltdown

Algunos Vendors y sus respectivos anuncios al respecto:

Vendor	Link
Intel	https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00088&languageid=en-fr
AMD	https://www.amd.com/en/corporate/speculative-execution
ARM	https://developer.arm.com/support/security-update
Microsoft	https://portal.msrc.microsoft.com/en-US/security-guidance https://support.microsoft.com/en-us/help/4073119/protect-against-speculative-execution-side-channel-vulnerabilities-in https://support.microsoft.com/en-us/help/4072698/windows-server-guidance-to-protect-against-the-speculative-execution https://support.microsoft.com/en-us/help/4073225/guidance-for-sql-server https://support.microsoft.com/en-us/help/4072699/important-information-regarding-the-windows-security-updates-released
RedHat	https://access.redhat.com/security/vulnerabilities/speculativeexecution
VMWare	https://lists.vmware.com/pipermail/security-announce/2018/000397.html
Apple	https://support.apple.com/en-us/HT208394
Google	https://googleprojectzero.blogspot.sk/2018/01/reading-privileged-memory-with-side.html

Con objeto de mantenerlo actualizado y protegido, quedamos a vuestra disposición para asesorarlo en cuanto a la detección de vulnerabilidades en su plataforma que puedan ser explotadas.

Obtenga mayor información sobre nuestros servicios y productos, póngase en contacto con nosotros:

Web: www.proactive.consulting

Mail: contacto@proactive.consulting

Tel: +595 (981) 478-921

Twitter: @ProActive_py