OPENLINK
SISTEMAS DE REDES DE DATOS

BOLETÍN SEGURIDAD

MELTDOWN Y SPECTRE, LAS NUEVAS VULNERABILIDADES DE LOS PROCESADORES

El Centro Nacional de Integración de Ciberseguridad y Comunicaciones (NCCIC) detectó un conjunto de vulnerabilidades de seguridad, conocidas como Meltdown y Spectre, que afectan a los procesadores informáticos modernos. La explotación de estas vulnerabilidades podría permitir a un atacante obtener acceso a información confidencial.

Meltdown: esta vulnerabilidad es la más fácil de explotar y la que obtiene la mayor atención. Afecta principalmente al chipset Intel y se trata actualmente con revisiones de nivel de sistema operativo de Microsoft, Apple y varias distribuciones de Linux. Funciona mediante el uso de un método llamado 'ejecución especulativa' para inferir valores en memorias protegidas. A esta vulnerabilidad se le ha asignado CVE-2017-5754.

Spectre: Este es un ataque más generalizado basado en conceptos similares a Meltdown y afecta a los procesadores Arm y AMD en formas que el ataque Meltdown no puede. Esto también significa que las soluciones para Meltdown no protegerán contra los ataques de Spectre. Spectre cubre dos vectores de ataque separados a los que se han asignado CVE-2017-5715 y CVE-2017-5753.

Si detecta algún evento de este tipo en su red, no dude en ponerse en contacto con el NOC/SOC de Openlink:

e-mail:
soc@oplk.com
mercadeo@oplk.com
Tel: 57 (1) 4321740 Ext. 574430
Cel: 57 (301)4866892

Los CVE de las vulnerabilidades son los siguientes:

CVE ID	CVSSv3 Vectors
CVE-2017-5754	5.6 Medium
CVE-2017-5715	5.6 Medium
CVE-2017-5753	5.6 Medium

Información sobre el sistema/producto afectado

Marca	Link
Intel	https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00088&languageid=en-fr
Microsoft	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV180002
Amazon	https://aws.amazon.com/de/security/security-bulletins/AWS-2018-013/
ARM	https://developer.arm.com/support/security-update
AMD	http://www.amd.com/en/corporate/speculative-execution
Google	https://googleprojectzero.blogspot.com.co/2018/01/reading-privileged-memory-with-side.html
MITRE	CVE-2017-5715 / CVE-2017-5753 / CVE-2017-5754
Red Hat	https://access.redhat.com/security/vulnerabilities/speculativeexecution
SUSE	https://www.suse.com/c/suse-addresses-meltdown-spectre-vulnerabilities/
CERT	http://www.kb.cert.org/vuls/id/584653
VMWare	https://www.vmware.com/us/security/advisories/VMSA-2018-0002.html
Apple	https://support.apple.com/en-us/HT208394

¿Qué impacto tendría si la vulnerabilidad es explotada?

- Aprovechando este fallo de seguridad un atacante podría tener acceso a información sensible alojada en la memoria del procesador (contraseñas, llaves de cifrado, etc).

¿Qué hacer si tenemos la vulnerabilidad?

- Microsoft recomienda actualizar los sistemas operativos Windows, y adicionalmente ha publicado procedimientos para ayudar a contrarrestar y verificar estas vulnerabilidades:

  Guía para usuarios Windows: https://support.microsoft.com/en-us/help/4073119/protect-against-speculative-execution-side-channel-vulnerabilities-in

  Guía para servidores Windows: https://support.microsoft.com/en-us/help/4072698/windows-server-guidance-to-protect-against-the-speculative-execution

Fuente:

https://www.us-cert.gov/ncas/alerts/TA18-004A

https://nvd.nist.gov

https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00088&languageid=en-fr

https://www.welivesecurity.com

https://www.trustwave.com/