UNIVERSIDAD DE COSTA RICA

CI Centro de Informática

08 de enero de 2018

Recomendaciones para protección de información ante vulnerabilidades Meltdown y Spectre

El Centro de Informática alerta a la comunidad universitaria sobre los ataques informáticos *Meltdown* y *Spectre*, vulnerabilidades de tipo hardware que están afectando procesadores Intel, AMD y ARM y que podrían comprometer información sensible y el espionaje de datos.

Con el fin de proteger los equipos institucionales ante estas amenazas, el Centro de Informática ha recopilado una serie de soluciones para los diversos sistemas operativos, que podrá consultar en el siguiente enlace:

http://apuntes.ucr.ac.cr/index.php/Vulnerabilidad_Meltdown_y_Spectre

Es obligatorio que cada responsable de equipo informático instale las actualizaciones correspondientes con el fin de proteger su información y eliminar las vulnerabilidades.

Para instalar dichas actualizaciones tomar en cuenta que el servidor local de actualizaciones Windows (WSUS) se encuentra al día y en sincronía con las últimas liberadas por Microsoft. Adicionalmente, a lo largo de esta semana estará liberado el acceso a Windows Update para que lo equipos que no están conectados a WSUS puedan actualizarse directamente desde Internet.

Por su parte, para dispositivos con Linux se han lanzado parches de seguridad para la vulnerabilidad de Meltdown mientras trabajan en una solución final para Spectre ya que presenta mayor complejidad. De igual forma, Apple lanzó una mitigación para Meltdown y trabaja en un solución para Spectre.

Finalmente, Android OpenSource Project ya cuenta con los parches de seguridad para ambas vulnerabilidades y dependerá de cada fabricante de dispositivos lanzar las actualizaciones para cada sistema.

Para más información, puede comunicarse al 2511-5000.

M.Sc. Alonso Castro Mattei

Director

MGA