

Seguridad relacionada con los productos de Canon con respecto a la vulnerabilidad de la CPU Meltdown y Spectre

CDMX, 16 de marzo de 2018.- Recientemente, las vulnerabilidades de CPU conocidas como Meltdown y Spectre se hicieron públicas.

Cuando el software malicioso es instalado en productos y ejecutado, estas vulnerabilidades pueden permitir el acceso a datos que generalmente serían inaccesibles.

En cuanto al impacto de estas vulnerabilidades en los productos de Canon, a partir de ahora, creemos que los productos y servicios que pueden verse afectados se enumeran a continuación.

- imagePRESS Server/ColorPASS/imagePASS. La empresa Electronics for Imaging Inc. (EFI) ha anunciado el estado de su respuesta en su página web:

<http://www.efi.com/support-and-downloads/kbarticle/article-details/?knowledgeArticleID=kA339000000HCDaCAO>

- imagePRESS CR Server.
- Canon Business Imaging Online MDS Cloud.
- Formularios en línea de Canon Business Imaging y servicios de impresión para Salesforce. El parche OS ha sido aplicado.

Aún estamos confirmando si los usuarios de estos productos se han visto afectados como resultado de estas vulnerabilidades. Sin embargo, para protegernos contra estas vulnerabilidades, estamos preparando medidas como parches de software, para garantizar que los usuarios puedan continuar utilizando los productos Canon con tranquilidad.

Actualmente no conocemos ningún otro producto de Canon que sea vulnerable a los métodos de ataque descritos de Meltdown y Spectre.

En caso de que se divulguen nuevos métodos de ataque relacionados con estas vulnerabilidades que, según determinemos, podrían afectar a los productos de Canon, actualizaremos esta información cuando sea necesario.

Para mayor información puede contactarnos directamente.



