



Concerniente al aviso de seguridad para las cámaras digitales de Canon relacionado con las funciones de comunicación a través del Protocolo de Transferencia de Imágenes (PTP) y las funciones de actualización del firmware.

5 de agosto de 2019.

Canon, Inc.

Gracias por usar los productos de Canon.

Un equipo internacional de investigadores de seguridad ha llamado nuestra atención sobre una vulnerabilidad relacionada con las comunicaciones a través del Protocolo de Transferencia de Imágenes (PTP), que es utilizado por las cámaras digitales de Canon, así como una vulnerabilidad relacionada con las actualizaciones de firmware.

(CVE-ID: CVE-2019-5994, CVE-2019-5995, CVE-2019-5998, CVE-2019-5999, CVE-2019-6000, CVE-2019-6001)

Debido a estas vulnerabilidades, existe la posibilidad de que terceros ataquen la cámara si se conecta a una PC o dispositivo móvil que ha sido usurpado a través de una red no segura.

En este momento, no existen casos confirmados de que estas vulnerabilidades hayan sido aprovechadas para causar daño, pero con el fin de asegurar que nuestros clientes puedan utilizar nuestros productos de forma segura, nos gustaría informarle de las siguientes soluciones para este problema.

- Asegúrese de que los ajustes de seguridad de los dispositivos conectados a la cámara, como la PC, el dispositivo móvil y el enrutador que se está utilizando, sean los adecuados.
- No conecte la cámara a una PC o dispositivo móvil que se esté utilizando en una red insegura, como en un entorno Wi-Fi gratuito.
- No conecte la cámara a una PC o dispositivo móvil que esté potencialmente expuesto a infecciones de virus.
- Desactive las funciones de red de la cámara cuando no se estén utilizando.
- Descargue el firmware oficial del sitio web de Canon cuando realice una actualización del firmware de la cámara.



Modelos afectados

Estas vulnerabilidades afectan las cámaras sin espejo y las cámaras SLR digitales de la serie EOS, PowerShot SX740 HS, PowerShot SX70 HS y PowerShot G5XMark II.

Actualización del firmware

Existe un mayor uso de PC y dispositivos móviles en un entorno de red inseguro (Wi-Fi gratuito) en el que los clientes no son conscientes de la seguridad de la red. Como ya es habitual transferir imágenes de una cámara a un dispositivo móvil a través de una conexión Wi-Fi, implementaremos actualizaciones de firmware para los siguientes modelos que están equipados con la función Wi-Fi.

Modelo	Disponibilidad de firmware estimada
EOS-1D X*1*2	Por determinar
EOS-1D X Mark II*1*2	Por determinar
EOS-1D C*1*2	Por determinar
EOS 5D Mark III*1	Por determinar
EOS 5D Mark IV	Por determinar
EOS 5DS*1	Por determinar
EOS 5DS R*1	Por determinar
EOS 6D	Por determinar
EOS 6D Mark II	Por determinar
EOS 7D Mark II*1	Por determinar
EOS 70D	Por determinar
EOS 80D	La versión 1.0.3 está disponible para descarga
EOS M10	Por determinar
EOS M100	Por determinar
EOS M3	Por determinar
EOS M5	Por determinar
EOS M50	Por determinar
EOS M6	Por determinar
EOS R	Por determinar
EOS RP	Por determinar
EOS Rebel SL2	Por determinar
EOS Rebel SL3	Por determinar
EOS Rebel T6	Por determinar
EOS Rebel T6i	Por determinar
EOS Rebel T6s	Por determinar
EOS Rebel T7	Por determinar
EOS Rebel T7I	Por determinar
EOS Rebel T100	Por determinar



PowerShot G5X Mark II	Por determinar
PowerShot SX70 HS	Por determinar
PowerShot SX740 HS	Por determinar

*¹Estos modelos requieren un adaptador Wi-Fi o un transmisor de archivos inalámbrico que sea compatible con la conectividad de Wi-Fi.

*²Las conexiones de Ethernet también pueden permitir estas vulnerabilidades.

La información de actualización de firmware se proporcionará para cada producto.

Muchas gracias,

Canon Mexicana S. de R.L. de C.V.

Información de contacto para consultas

Centro de Asistencia al Cliente de Canon

Ciudad de México y Área metropolitana: 55 52 49 49 05

Interior de la República: 800 710 7168

Correo electrónico: canonmx_soporte@cusa.canon.com

Para conocer opciones adicionales de asistencia: www.canon.com.mx/servicio/contactanos