Acerca de la vulnerabilidad en el protocolo de encriptación Wi-Fi WPA2

8 de diciembre de 2017

Canon Inc.

Recientemente, un investigador hizo pública la vulnerabilidad conocida como KRACK en el protocolo de encriptación estándar WPA2 para redes LAN inalámbricas (Wi-Fi). Esta vulnerabilidad permite que un atacante intercepte, de manera intencional, la transmisión inalámbrica entre el cliente (terminal equipada con la funcionalidad Wi-Fi) y el punto de acceso (el enrutador, etc.) para realizar actividades potencialmente maliciosas. Por esta razón, esta vulnerabilidad no puede ser explotada por otros fuera del rango de la señal de Wi-Fi, ni por otros en ubicaciones remotas que usen la internet como intermediario.

Aún debemos confirmar si los usuarios de los productos Canon han sufrido inconvenientes como resultado de esta vulnerabilidad; sin embargo, para permitir que los clientes continúen usando nuestros productos con tranquilidad, recomendamos poner en práctica las siguientes medidas preventivas:

- Use un cable USB o cable Ethernet para conectar los dispositivos compatibles directamente a una red
- Encripte la transmisión de datos desde los dispositivos que permitan las configuraciones de encriptación (TLS/IPSec)
- Use medios físicos como tarjetas SD con los dispositivos compatibles
- Use configuraciones tales como Wireless Direct y Direct Connect con los dispositivos compatibles

*Debido a que las funciones y los procedimientos de operación ofrecidos pueden variar dependiendo del dispositivo utilizado, le agradecemos consulte la información del manual de su dispositivo para conocer más detalles.

*También recomendamos que tome las medidas apropiadas para aquellos dispositivos como su PC o teléfono inteligente. Para cono cer la información acerca de las medidas apropiadas para cada dispositivo, le agradecemos se comunique con el fabricante del equipo.

Información de contacto para las consultas

Si poseen alguna consulta sobre el anuncio, por favor contáctenos directamente.