Regarding the vulnerability in WPA2 Wi-Fi encryption protocol

December 8, 2017

Canon Inc.

Recently, a researcher made public a vulnerability known as KRACKs in the standard wireless LAN (Wi-Fi) encryption protocol WPA2. This vulnerability allows an attacker to intentionally intercept the wireless transmission between the client (terminal equipped with Wi-Fi functionality) and the access point (the router etc.) to perform potentially malicious activity. For that reason, this vulnerability cannot be exploited by anyone outside the range of the Wi-Fi signal or by anyone in a remote location using the internet as an intermediary.

We have yet to confirm that any issues have been encountered by users of Canon products as a result of this vulnerability, however, in order to allow customers to continue using our products with peace of mind, we recommend the following preventative measures:

- Use a USB cable or Ethernet cable to directly connect compatible devices to a network
- Encrypt data transmission from devices that enable encryption settings (TLS/IPSec)
- Use such physical media as SD cards with compatible devices
- Use such settings as Wireless Direct and Direct Connect with compatible devices

*As the operation procedures and functions offered vary from device to device, please consult your device's manual for more details.

*We also recommend you take appropriate measures for such devices as your PC or smartphone. For information on the appropriate measures for each device, please contact the device's manufacturer.

Contact Information

Should you have any questions about this notice, you may contact us directly.