Support and Downloads

General

8 December 2017

Vulnerability in WPA2 Wi-Fi encryption protocol

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 updated our product support sites to provide our customers with information on proper safeguards to mitigate risks associated with this vulnerability.

- Office Multi-function printers, small office multi-function printers, production printers, and laser beam printers
- Camera, camcorders, projectors, compact photo printers
- Large format printers
- Inkjet printers, inkjet multi-function printers

For products not covered above, please contact your nearest service centre .

Canon regards the secure and safe use of our products as a matter of high importance to ensure that our customers have full confidence when using our products.