NOTICE

SDHC/SDXC MEMORY CARD WITH EMBEDDED WIRELESS LAN FUNCTIONALITY FLASHAIR MAY HAVE A SECURITY VULNERABILITY RELATED TO THE GENERATION AND MANAGEMENT OF WPA2 KEY

17 OCTOBER 2017

Toshiba Memory Corporation

To: Valued Customers,

Toshiba Memory Corporation is informing our valued customers of a potential WPA2 wireless LAN protocol vulnerability with the Toshiba Memory FlashAir™ ("Product") has been identified. This vulnerability is related to the generation and management of key information which is utilized for encrypting data. With this vulnerability there exists a possibility that the data transmitted between the Product and wireless LAN devices such as smartphone can be compromised.

The WPA2 is used widely for wireless LAN. We have discovered that this behavior exists when the FlashAir™ W-04 ("Software Update Affected Product") is used in "Internet pass thru" mode. Therefore, **please do not connect the Software Update Affected Product* using the wireless LAN "Internet pass thru" mode until the software has been updated** (mentioned below). **To correct this issue we are now in the process of addressing this vulnerability via a software update which is expected to be released on or before the end of December, 2017. Please update the software when it is released.** Even if "Internet pass thru" mode is disabled on the Software Update Affected Product*, the device connected to it could exhibit this vulnerability and transmitted data could still be compromised.

We also ask customers to check this vulnerability of the Devices prior to connecting to the FlashAir™ W-03, FlashAir™ W-02 and FlashAir™ Class6 as well as the Software Update Affected Product. About the vulnerability of the Devices, please contact to Devices' customer and/or technical support.

If you have any questions about this vulnerability of the Product, please contact your local technical support representative and we will be happy to support you. For information regarding how to reach your local technical support representative, please visit http://www.toshiba-personalstorage.net/ww/support/index.htm."

Software Update Affected Product Information

Software Update Affected Product	Model	Capacity Label
 SDHC/SDXC Memory Card with embedded wireless LAN functionality FlashAir™ W-04	THN-NW04W0640A6	64GB
	THN-NW04W0320A6	32GB
	THN-NW04W0160A6	16GB

*Note: “Internet pass thru” mode is disabled by default on the FlashAir™ W-04.

EXPLANATION OF THE VULNERABILITY

Toshiba Memory Corporation as found a vulnerability of the WPA2 protocol used for wireless LAN encryption. This vulnerability is related to the generation and management of key information that encrypts the data transmitted.

VULNERABILITY THREAT

There exists the possibility that data transmitted between the FlashAir™ W-04 and a wireless device may be compromised.

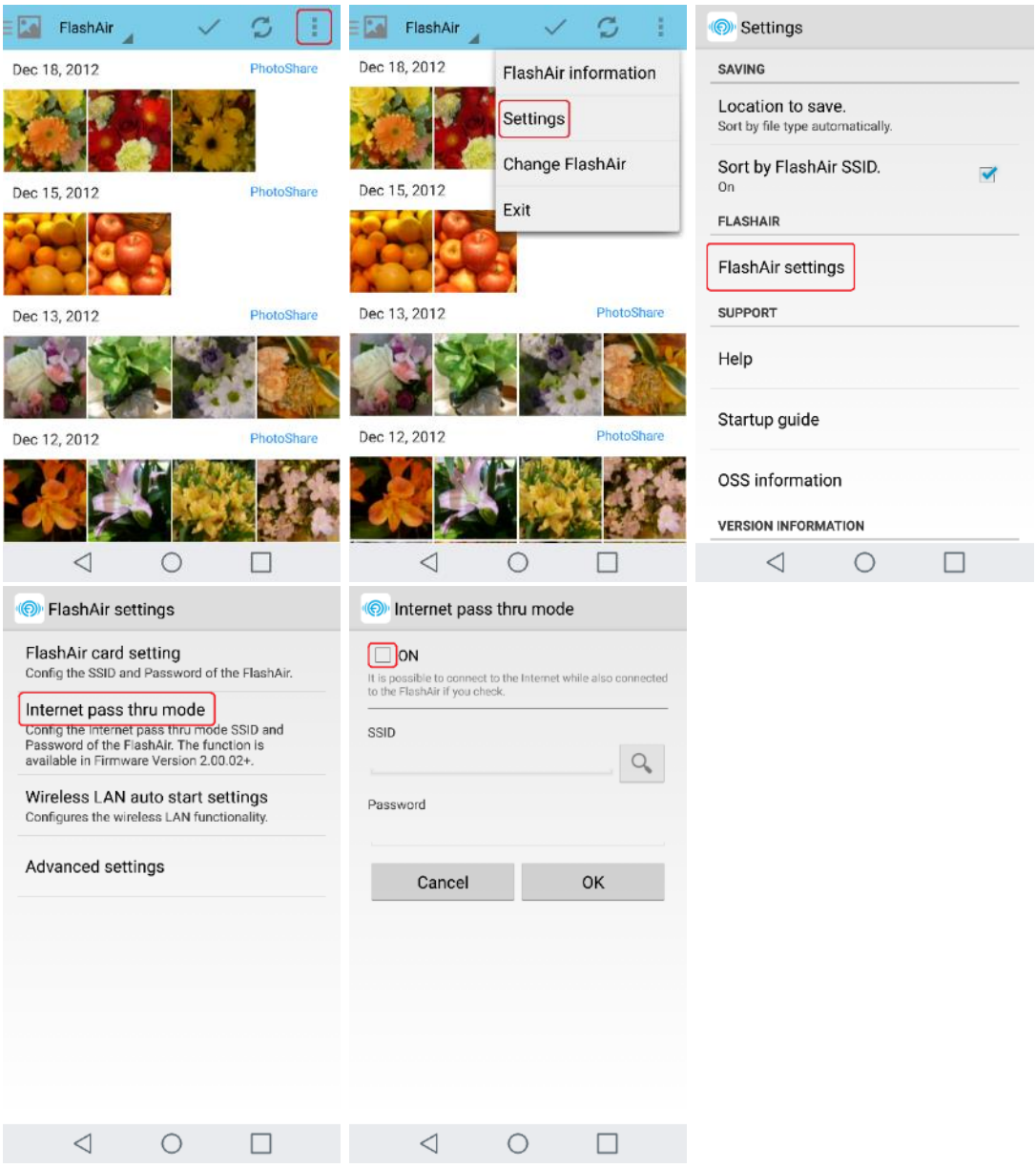
WORKAROUND

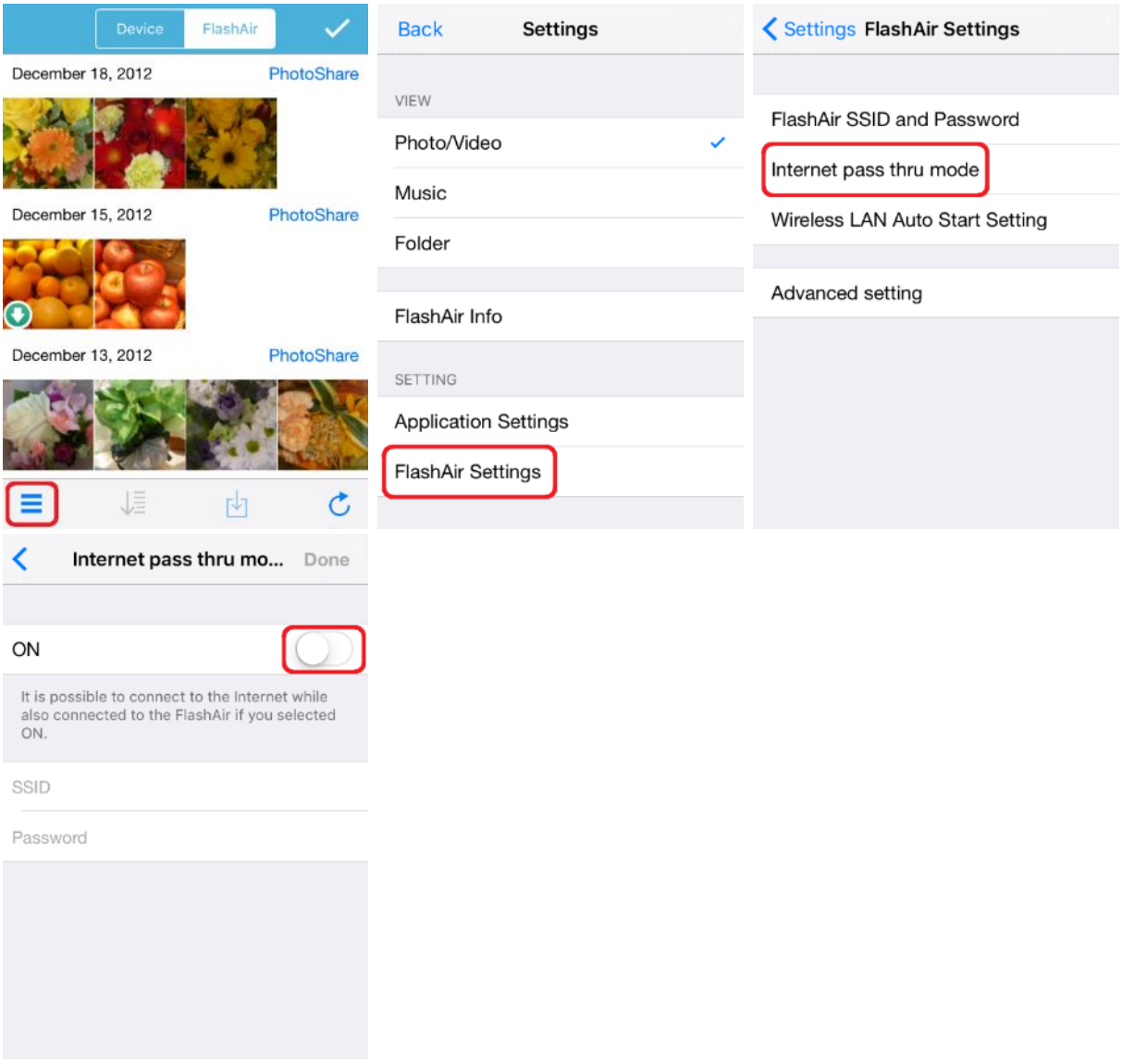
A Software update will be released on or before the end of December, 2017. Until this new software has been released, please disable “Internet pass thru” mode on the FlashAir™ W-04. Note: “Internet pass thru” mode is disabled by default on the FlashAir™ W-04.

“Internet pass thru” mode can be disabled by using the FlashAir iOS or Android™ App or FlashAir Configuration Software, and following these steps:

In the case of FlashAir iOS and Android™ App, while connecting to Wi-Fi network to FlashAir™, open “Settings” > “FlashAir settings”> “Internet pass thru mode” and then you can check and/or change the mode.

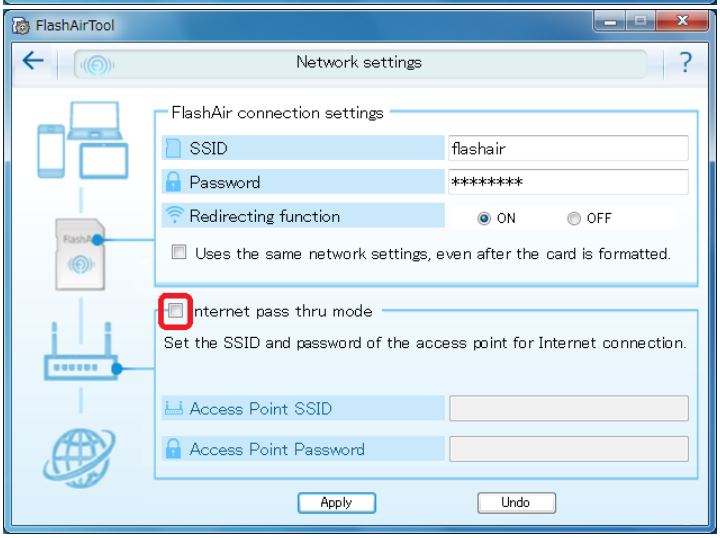
If you are prompted to enter "MASTERCODE", enter the "MASTEROCDE".





In the case of FlashAir Configuration Software

Insert the FlashAir into a PC. Open "FlashAir Configuration Software" > "Network settings." and then you can check and/or change the mode.



* WPA2 is a trademark of Wi-Fi Alliance.

* Android is a trademark of Google Inc.

*All other company names, product names, and service names may be trademarks of their respective companies