NOTICE

CANVIO AEROMOBILE WIRELESS SSD

17 OCTOBER 2017

VULNERABILITY FOUND RELATED TO THE GENERATION AND MANAGEMENT OF WPA2 KEY

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 Canvio AeroMobile Wireless SSD 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 Canvio AeroMobile Wireless SSD and wireless LAN devices can be compromised.

The WPA2 is used widely for wireless LAN. We have discovered that this behavior exists when the Canvio AeroMobile is used in "Station" mode. Therefore, **please do not connect the Canvio AeroMobile Wireless SSD using the wireless LAN "Station" mode until the firmware has been updated** (mentioned below). Even if "Station" mode is disabled on the Canvio AeroMobile Wireless SSD*, the device connected to it could exhibit this vulnerability and transmitted data could still be compromised if such connected device is in "Station" mode.

To correct this issue, we are now in the process of addressing this vulnerability via a firmware update which is expected to be released on or before November 30, 2017. Please update the firmware when it is released.

We also ask customers to check this vulnerability of the Devices prior to connecting to the Canvio AeroMobile Wireless SSD. About the vulnerability of the Devices, please contact to Devices' customer and/or technical support. If you have any questions about this vulnerability of Canvio AeroMobile Wireless SSD, 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 www.toshibastorage.com."

*Note: "Station" mode is disabled by default on the Canvio AeroMobile Wireless SSD.

Product Information

Product Name
Toshiba Canvio AeroMobile Wireless SSD

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 Canvio AeroMobile Wireless SSD and a wireless device may be compromised.

WORKAROUND

A firmware update will be released on or before November 30, 2017. Until this new firmware has been released, please disable “Station” mode on the Canvio AeroMobile Wireless SSD. Note: “Station” mode is disabled by default on the Canvio AeroMobile.

“Station” mode can be disabled by using the Canvio AeroMobile IOS and Android App, and following these steps:

1. Please select the “Setting” button (Upper right of the screen.).

2. Then select the “Internet” button and choose the connected access point.

3. Then select the “Forget” button.