17 October 2017

NOTICE

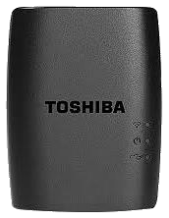
Vulnerability found related to the generation and management of WPA2 Key on CANVIO (STOR.E) wireless products

Toshiba Electronic Devices & Storage Corporation

To: Valued Customers,

Toshiba Electronic Devices & Storage Corporation is informing our valued customers of a potential WPA2 wireless LAN protocol vulnerability with the Canvio Wireless Adapter in addition to the Canvio AeroCast as ones of the Canvio (STOR.E) Wireless products 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 AeroCast and/or the Wireless Adapter (the “Wireless Product”) and wireless LAN devices can be compromised.
New firmware that fixed this vulnerability becomes available. So, please be sure to apply firmware update of the Wireless Product provided in “Firmware update” section later.

Product Information

Product Name (varied at location)	**Model No.**	**Product image**	**Firmware version**
Canvio AeroCast / Canvio AeroCast wireless HDD	HDTU110*KWC1		1.2.6 and earlier
Canvio Wireless Adapter / STORE.E Wireless Adapter / Canvio CAST Wireless Adapter	HDWW100*KW*1		2.0.5 and earlier

We also ask customers to check this vulnerability of the other your wireless devices prior to connecting to/from the Wireless Product.

About the vulnerability of your wireless devices, please contact to devices’ support center. If you have any questions about this vulnerability of the Wireless Product, please contact your local support center representative and we will be happy to support you.

Explanation of the Vulnerability

Toshiba Electronic Devices & Storage 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 Toshiba Wireless Product and wireless LAN devices may be compromised.

Firmware update

1. Canvio AeroCast

   Please be sure to download the user manual to your PC or Mac and read carefully the user manual before downloading firmware.

   Please download firmware to your PC or Mac, and then update firmware following to the manual.

Firmware Version	Release Date	Firmware	Manual
1.2.8	22 Dec 2017	> Download	>PDF :1.19MB

2. Canvio Wireless Adapter

   Please be sure to download the user manual to your PC or Mac and read carefully the user manual before downloading firmware.

   Please download firmware to your PC or Mac, and then update firmware following to the manual.

Firmware Version	Release Date	Firmware	Manual
2.0.7	22 Dec 2017	>Download	>PDF : 592KB

Vulnerability Related Information

Japan Vulnerability Notes (JVN)

Contact Us

Please visit the following website and choose Consumer Storage Solutions website in your region.

Toshiba Storage