

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 AeroCast as one 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 wireless LAN devices can be compromised.

The WPA2 is used widely for wireless LAN. We have discovered that this behavior exists when the Canvio AeroCast is used at connecting to the internet in both the "Station" and the "Bridge" mode. Therefore, **please do not connect it to the internet.**

If you have connected the Canvio AeroCast to the internet before, please RESET it as described below. Also please connect the Canvio AeroCast with your wireless devices without connecting to the internet.

To correct this issue, we are now in the process of addressing this vulnerability.

Product Information

Product Name(varied at location)	Model No.	Product image
Canvio AeroCast / Canvio AeroCast wireless HDD	HDTU110*KWC1	

We also ask customers to check this vulnerability of the Devices prior to connecting to the Canvio AeroCast / Wireless Adapter*. About the vulnerability of the Devices, please contact to Devices' support center. If you have any questions about this vulnerability of the Canvio AeroCast / Wireless Adapter*, please contact your local support center representative and we will be happy to support you.

*Below is product image of the Wireless Adapter.



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

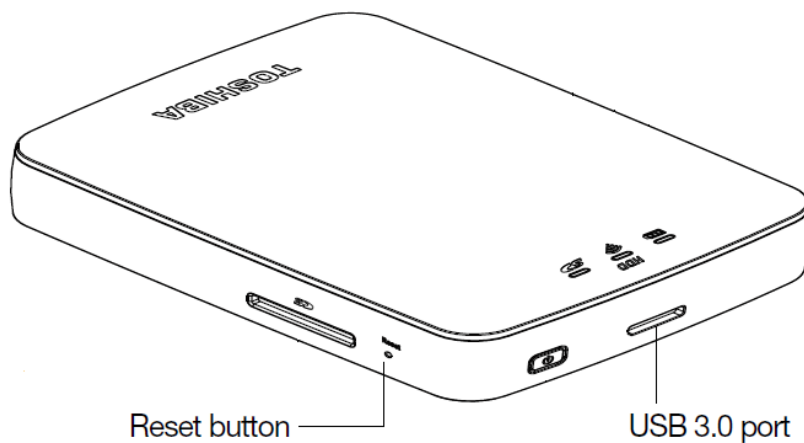
There exists the possibility that data transmitted between the Canvio AeroCast and wireless LAN devices may be compromised.

Workaround

1. At first, **please do not connect to the internet.**

After power on, please do not connect to the internet via application. If connected, there exists a possibility that the data transmitted can be compromised.

2. If you have connected the Canvio AeroCast to the internet regardless the "Station" or the "Bridge" mode, please RESET the Canvio AeroCast.



- After power-on and press and hold Reset button for 5 seconds in Wireless LAN mode. The system will restore to its factory settings. Please configure settings again as needed.

3. Please connect the Canvio AeroCast with your wireless devices without connecting to the internet.

Vulnerability Related Information

[Japan Vulnerability Notes \(JVN\)](#)

Contact

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

[Toshiba Storage](#)