

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.

The vulnerability is exposed when the Wireless Product is used to connect to the internet in either the "Station" or the "Bridge" mode. Therefore, we strongly urge **you not to connect the Wireless Product to the internet.**

If you have connected the Wireless Product to the internet, please immediately RESET it as described below. Until further notice, when connecting the Wireless Product to your wireless devices, please ensure doing so 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	
Canvio Wireless Adapter / STORE.E Wireless Adapter / Canvio CAST Wireless Adapter	HDWW100*KW*1	

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

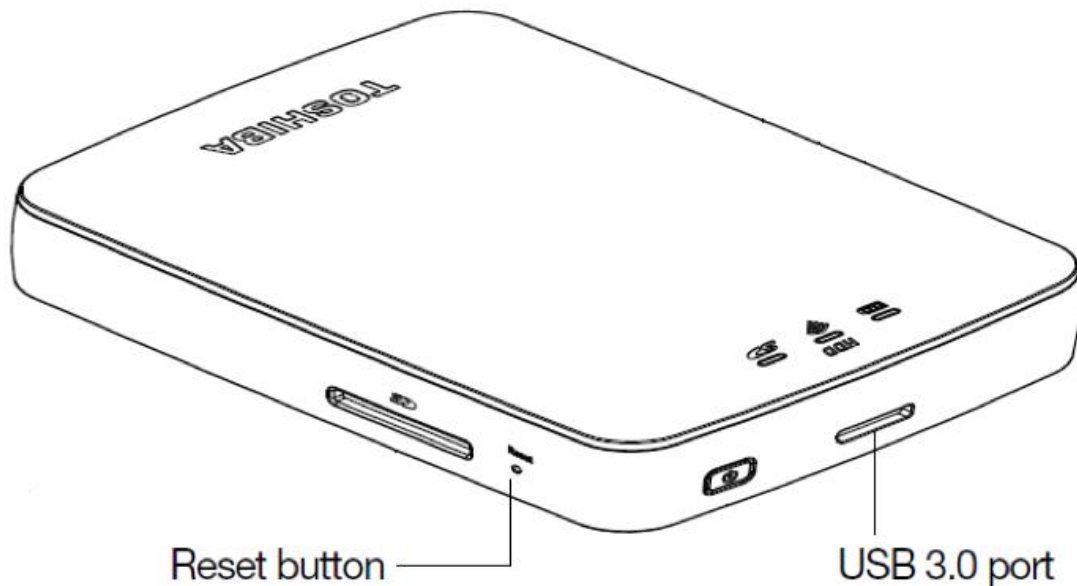
There exists the possibility that data transmitted between the Toshiba Wireless Product and wireless LAN devices may be compromised.

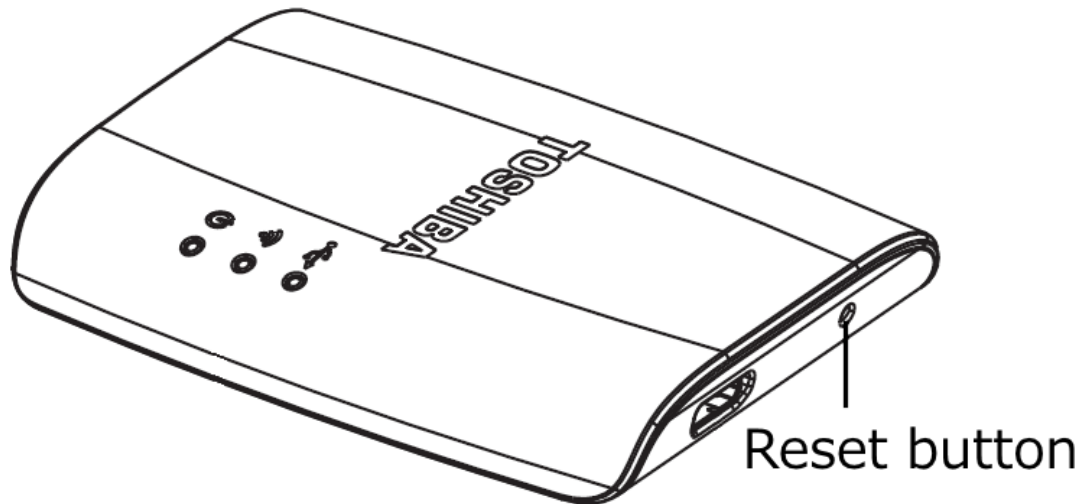
## Workaround

1. If the Wireless Product has never been connected to the internet, please continue to avoid doing so.

Specifically, after power on the Wireless Product, please do not connect to the internet via application. If connected to the internet, there exists a risk that the data transmitted will be compromised.

2. If the Wireless Product has been or is connected to the internet, regardless of whether the "Station" or the "Bridge" mode was/is used, please RESET the Wireless Product, as discussed below.





- 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 without connecting to the internet.

3. Please connect the Wireless Product to your wireless devices without connecting to the internet to prevent exposing the vulnerability described above.

## 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](#)