July 26, 2018

TDSCSA00436: Multiple Vulnerabilities in CANVIO Network Storage Products

Toshiba Electronic Devices & Storage Corporation

■Overview

There are multiple vulnerabilities including remote arbitrary code execution in the CANVIO (STOR.E) wireless products, if these products or connected devices are connected to the internet. To mitigate these vulnerabilities you should follow below instructions.

■Affected Network Storage Products

Product Category	Product Name (varies by location)	Model No.	Firmware Version
Wireless products	CANVIO AeroCast / CANVIO AeroCast Wireless HDD	HDTU110*KWC1	1.2.8 or earlier
	CANVIO Wireless Adapter / STOR.E Wireless Adapter	HDWW100*KW*1	2.0.7 or earlier

Note: The asterisk mark (*) represents an alphanumeric character.

■Impacts

OSS modules in the Affected Network Storage Products, including samba, have vulnerabilities including CVE-2017-7494. The details are shown in the following "Vulnerability Information for each OSS Module List".

These vulnerabilities can allow remote attackers to cause information leakage / modification, and to potentially take control of the Affected Network Storage Products.

Please understand that the impacts may occur, if you use the Affected Network Storage Products or devices connected to these products with an internet connection.

<Vulnerability Information for OSS Module List>

■Workarounds

Please use the product and also connected devices without internet connection.

Connection types	
Via home broadband network	Set Wireless Product up to AP mode. Disconnect devices connected to the Wireless Product from the internet. *1 *2
Via wireless LAN	1. Update the latest firmware that fixed WPA2 vulnerabilities of Wireless product. 2. Change the default password to a unique password. 3. Disconnect devices connected to the Wireless Product from the internet.
Via mobile broadband network (smartphone, tablet, WWAN-equipped PC, etc.) *3	Disconnect from WWAN *3 Disconnect devices connected to the Wireless Product from the internet.

*1: Please be sure to download the user manual (see links in the table below) and read it carefully prior to setup.

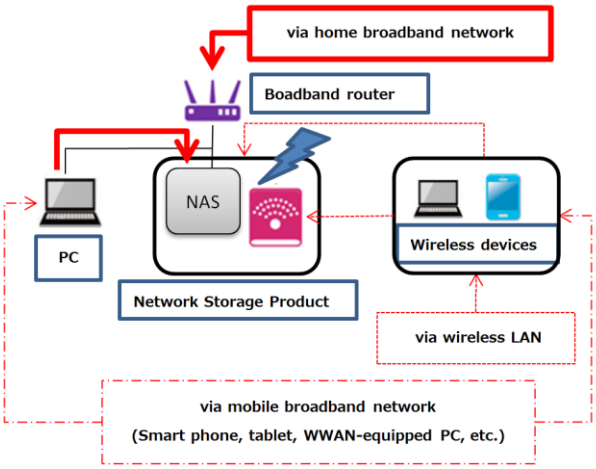
*2: Please be sure to update the latest firmware that addressed WPA2 vulnerabilities.

*3: WWAN means “Wireless Wide Area Network”.

Note 1: Toshiba Electronic Devices & Storage Corporation terminates the software update for the Affected Network Storage Product.

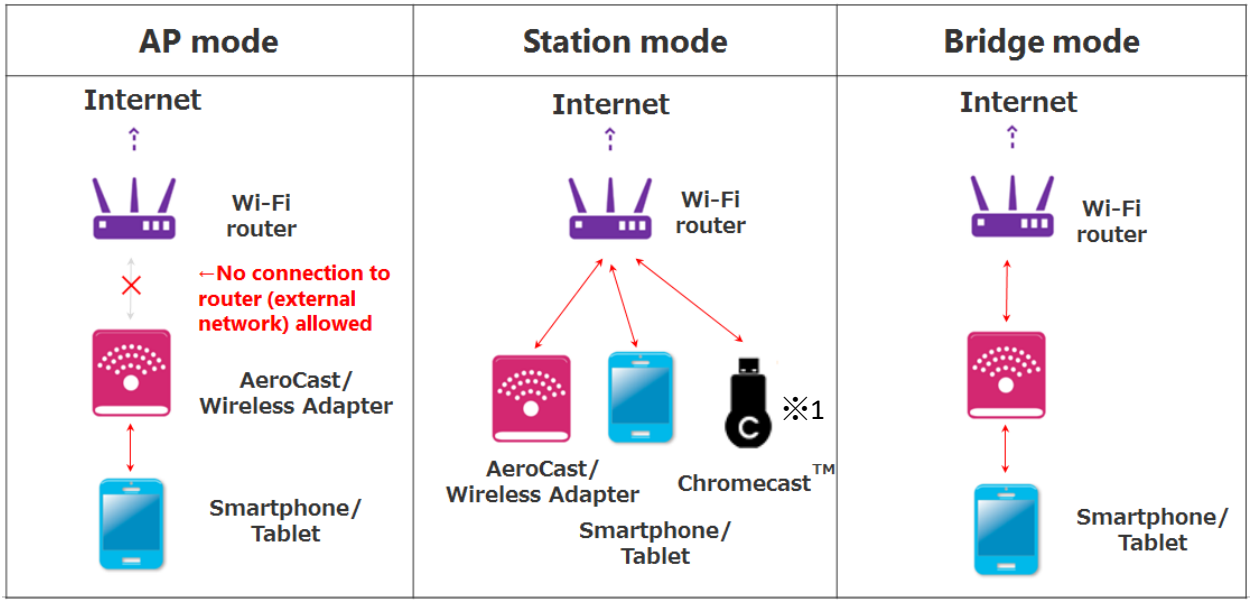
Note 2: Please be sure to apply the appropriate firmware update according to the information provided by the manufacturer of any devices that are connected to the Affected Network Storage Product.

<Attack Routes>



■Different Connection Modes

Please use AP (access point) mode and disconnect connected devices from the internet to mitigate impacts of vulnerability. Please be aware that it is possible that in station and bridge mode vulnerabilities can occur.



※1:You cannot use Chromecast™ function after the setup".

※ Chromecast is trademark of Google, Inc.

Product Name	Manual
CANVIO AeroCast / CANVIO AeroCast Wireless HDD	https://www.toshiba-storage.com/wp-content/uploads/2018/05/UM_Canvio_AeroCast.pdf
CANVIO Wireless Adapter / STOR.E Wireless Adapter	https://www.toshiba-storage.com/wp-content/uploads/2018/05/UM_STORE_Wireless_Adapter.pdf

■ Reference

・The latest firmware to address WPA2 vulnerability:

http://www.canvio.jp/en/news/hdd/ot_notice/20171017.htm

・ Common Vulnerability Scoring System SIG:

https://www.first.org/cvss/

・Software Update Termination for CANVIO Network Storage Products:

https://www.toshiba-storage.com/wp-content/uploads/2018/07/Toshiba_Software_Update_Termination_072018.pdf

■Contact Information

https://www.toshiba-storage.com/contact/