July 20, 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 and NAS products (the “Affected Network Storage Product”). Please stop using them or apply the workarounds so that these may mitigate the impact of these vulnerabilities.

■Affected Network Storage Products

Product Category	Product Name (varied 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 / CANVIO Cast Wireless Adapter	HDWW100*KW*1	2.0.7 or earlier
NAS products	CANVIO PERSONAL CLOUD / CANVIO HOME	HDNB1*0*E*1	0011.3050 or earlier

Note: An asterisk mark (*) is an alphanumeric character.

■Impact

OSS modules in the Affected Network Storage Products, including samba, have known vulnerabilities including CVE-2017-7494. The details are shown in the following “Vulnerability Information for each OSS module list ”.

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

<Vulnerability Information for each OSS module list>

■Workarounds

・Please understand that the impact may occur if you continue to use the Affected Network Storage Products.

・The following workarounds may mitigate the impact of these vulnerabilities in the Affected Network Storage Products.

Connection types	Method to mitigate the impact of these vulnerabilities	
	NAS product	Wireless product
Via home broadband network	Filter traffic related to the vulnerabilities using a firewall device, such as a broadband router.	Set Wireless product up to AP mode. *1 *2
Via wireless LAN	Confirm that there are no wireless communication devices within your local network.	1. Update the latest firmware that fixed WPA2 vulnerabilities of Wireless product. 2. Change the default password to a unique password.
Via mobile broadband network (smart phone, tablet, WWAN-equipped PC, etc.) *3		Disconnect from WWAN *3

*1: Please be sure to download the user manual and read it carefully prior to setup.

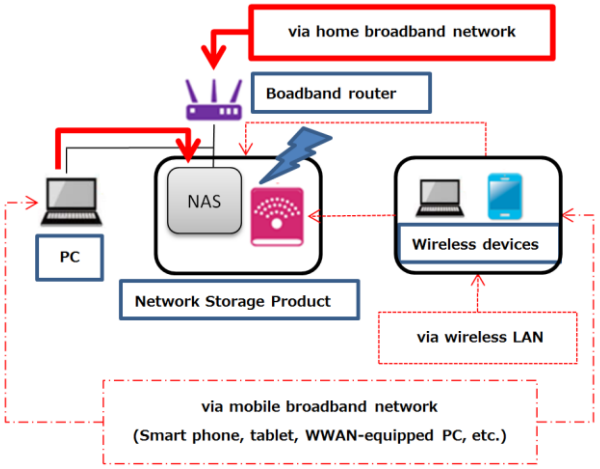
*2: Please be sure to update the latest firmware that addressed WPA2 vulnerabilities.

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

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

Note: 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 route>

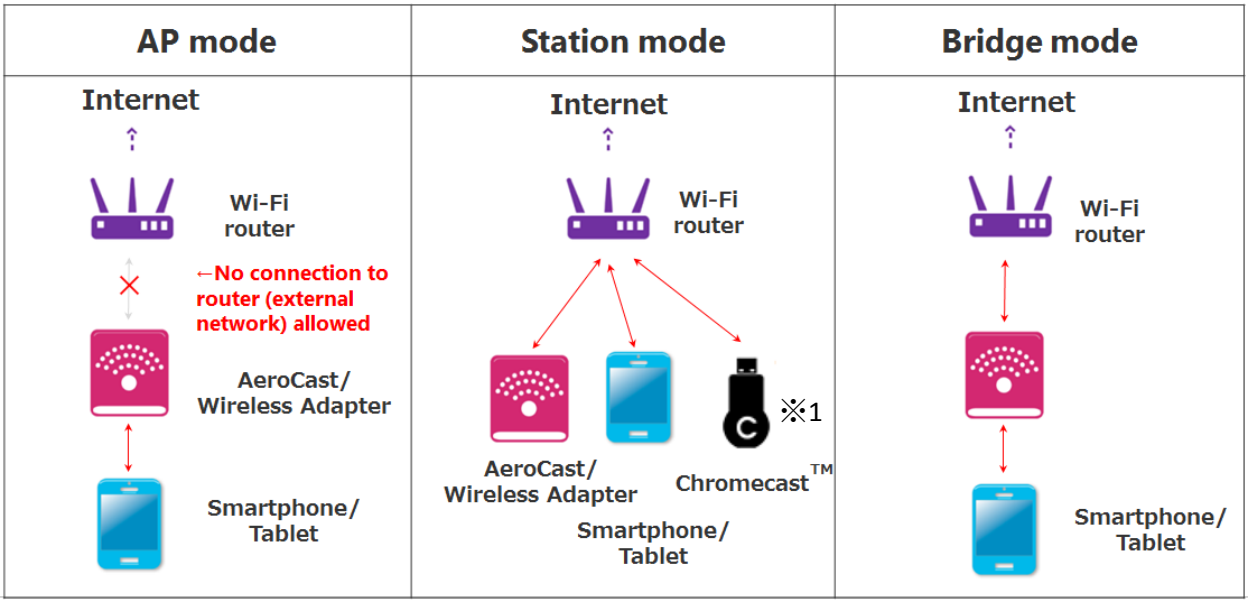


<Wireless products>

Different connection modes

・Use the “AP mode” (shown below) to mitigate the impact of these vulnerabilities.

・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	> Download
CANVIO Wireless Adapter / STOR.E Wireless Adapter / CANVIO Cast Wireless Adapter	> Download

■ Reference

・The latest firmware to address WPA2 vulnerability

・ Common Vulnerability Scoring System SIG

・”Software Update Termination for CANVIO Network Storage Products”

■Contact Information

https://storage.toshiba.com/consumer-hdd/support/contact