TOSHIBA
Leading Innovation

TDSCSA00358: Default Password Vulnerability in CANVIO (STOR.E) wireless products

Feb. 28, 2018

■ Overview

It has been reported that there may be default password vulnerability in the CANVIO (STOR.E) wireless products.

Please be sure to change the default password upon your initial use of the CANVIO (STOR.E). If you do not change the default password there is a possibility that an unknown person may utilize the wireless communications range of the CANVIO (STOR.E) and may access the entire shared file system.

■ Affected Product

Product Name (varied at location)	Model No.	Product Image	Vulnerability
Canvio AeroCast / Canvio AeroCast wireless HDD	HDTU110*KWC1		Default Password
Canvio Wireless Adapter / STORE.E Wireless Adapter / Canvio CAST Wireless Adapter	HDWW100*KW*1		Null Default Password

TOSHIBA
Leading Innovation

■Threats for each model:

Model No.	Threats
HDTU110*KWC1	An unknown person within the wireless communications range of an affected product with knowledge of the default password may access the entire shared file system in the product without restriction.
HDWW100*KW*1	An unknown party within the wireless communications range of an affected product may access the entire shared file system in the product without restriction.

■Countermeasures

Change or set the password

Immediately change and replace the default password upon first usage of the product with a sufficiently strong and unique password.
See US-CERT Security Tip ST04-002 and Password Security, Protection, and Management for more information on password security.

TOSHIBA
Leading Innovation

Counter measure for each model:

Model No.	Countermeasure
HDTU110*KWC1	Please be sure to change the default password immediately upon first usage of the product. To set your unique password, please refer to this user manual and the FAQs on your applicable regional support site. The default password is automatically set upon shipping of the product. Even if the default password is changed to your unique password, your unique password may be reset to a default password in the following situations: 1. When the user resets the product by using the associated App or by depressing the Reset button to accomplish a reset. 2. When the option “Enable factory default after firmware upgrade” is selected and the user updates the firmware.
HDWW100*KW*1	Please be sure to enable and set your unique password immediately upon first usage of the product. To set your unique password, please refer to this user manual and the FAQs on your applicable regional support site. The default password is null upon shipping of the product. Even if your unique password is set, your unique password will be reset in the following situations: 1. When the user resets the product by using the associated App or by depressing the Reset button to accomplish a reset. 2. When the option “Enable factory default after firmware upgrade” is selected and the user updates the firmware.

TOSHIBA
Leading Innovation

■ References

Alert (TA13-175A) Risks of Default Passwords on the Internet

https://www.us-cert.gov/ncas/alerts/TA13-175A

■ Revision History

Feb. 28 2018 Date revision published.

■ Contact Information

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

http://www.toshiba-personalstorage.asia/contact/