

TMCSA00315: Default Password Vulnerability in CANVIO AeroMobile Wireless SSD

Date First Published: Feb. 28, 2018

■ Overview

It has been reported that there may be default password vulnerability in the CANVIO AeroMobile Wireless SSD.

Please be sure to change the default password upon your initial use of the CANVIO AeroMobile Wireless SSD. 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 AeroMobile Wireless SSD and may access the entire shared file system.

■ Affected Product

Product Name	Model No.	vulnerability
CANVIO AeroMobile Wireless SSD	HDTQ112*	Default Wi-Fi Password, Default Admin Password

■ Threats for each model:

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.

■ 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.

Countermeasure:

Please be sure to change the default Wi-Fi password and the default Admin password immediately upon first usage of the product. To set your unique password, please refer to this user manual 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 situation:

In case the product is reset by depressing the Reset button to accomplish a reset of the product.

■ 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.

If you have any questions about this vulnerability of Canvio AeroMobile Wireless SSD, please contact your local technical support representative. For information regarding how to reach your local technical support representative, please visit www.toshibastorage.com.