TMCSA00317: Multiple Vulnerabilities and Software Update Termination for CANVIO AeroMobile Wireless SSD

Date First Published: Aug. 30, 2018

■ Overview

Toshiba Memory Corporation is informing our valued customers of potential multiple vulnerabilities with Toshiba Canvio AeroMobile Wireless SSD have been identified. The multiple vulnerabilities include remote arbitrary code execution in Canvio AeroMobile Wireless SSD.

We ask customers to apply the workaround to mitigate the impact of these vulnerabilities.

Toshiba Memory Corporation is also informing about the termination of the further software update of Canvio AeroMobile Wireless SSD.

■ Affected Product

Product Name
Toshiba Canvio AeroMobile Wireless SSD

■ Vulnerability Threat

OSS modules in the Affected Products, such as samba, have known vulnerabilities including, but not limited to CVE-2012-1182. The details that we acknowledged are shown in the following “Vulnerability Information list for OSS modules”.

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

<Vulnerability list of OSS modules>

OSS Name	Version	Example of CVEs	CVSS v2.0
samba	3.0.24	CVE-2012-1182	10
ez-ipupdate	3.0.10	CVE-2004-0980	10
ffmpeg	0.6.1	CVE-2013-4265	10
sqlite	3.7.13	CVE-2015-5895	10

libpng	1.2.44	CVE-2015-8540	9.3
pcre	7.9	CVE-2015-8391	9
linux_kernel	2.6.36	CVE-2017-1000251	8.3
busybox	1.12.1	CVE-2016-6301	7.8
ntp	4.2.4p2	CVE-2015-7701	7.8
dnsmasq	2.22	CVE-2017-14496	7.8
lighttpd	1.4.28	CVE-2013-4599	7.6
iptables	1.4.10	CVE-2012-2663	7.5
libexif	0.6.20	CVE-2012-2840	7.5
libFLAC	1.2.1	CVE-2014-9028	7.5
tiff	4.0.3	CVE-2018-5360	6.8
e2fsprogs	1.39	CVE-2007-5497	5.8
U-Boot	1.1.3	CVE-2017-3225	5.6
libid3tag	0.15.1b	CVE-2004-2779	5

■ Workaround

Please disable “Station” mode on the Canvio AeroMobile Wireless SSD.

Note: “Station” mode is disabled by default on the Canvio AeroMobile.

“Station” mode can be disabled by using the Canvio AeroMobile iOS and Android App, and following these steps:

1. Please select the “Setting” button (Upper right of the screen.).
2. Then select the “Internet” button and choose the connected access point.
3. Then select the “Forget” button.

■ References

VULNERABILITY FOUND RELATED TO THE GENERATION AND MANAGEMENT OF WPA2 KEY
https://storage.toshiba.com/docs/support-docs/toshiba_canvio_aeromobile_wireless_ssd_wpa2_hack_rev_6_01.pdf?sfvrsn=bc3669fe_4

TMCSA00315: Default Password Vulnerability in CANVIO AeroMobile Wireless SSD
https://toshiba.semicon-storage.com/content/dam/toshiba-ss/ncsa/en_us/docs/services-support-documents/Security_Advisory_Default_PW_2018016_%20AeroMobile.pdf

■ Revision History

Aug. 30 2018 New released.

■ Contact Information

If you have any questions about this vulnerability of Canvio AeroMobile Wireless SSD, please contact your local technical support representative and we will be happy to support you. For information regarding how to reach your local technical support representative, please visit "www.toshibaMemoryCorp.com."