Product Management Info – PMI

Commercial Avionics

▶ Original Date: March 3rd, 2018
Updated Date: September 3rd, 2018

PMI #	142
Division	Commercial Avionics
Location/Site	San Diego, CA
Notice Type	Product Change Notification
Product(s)	73001011-xxx
Product Manager	RJ McLaren
Intended Audience	All Customers

▶ A100 Cab-n-Connect – Product Change Notification

The intention of this notification is to inform customers who buy the A100 Cab-n-Connect product that Kontron will be implementing a WiNG firmware update to the product line.

The reasons for the WiNG firmware update are as follows;

- KRACK, WPA2 Protocol Flaw Vulnerability (see further information below)
  - The update has the 802.11r and Group Key Rotation disabled without the option of enabling
- WiNG crashes in the DIAG prompt mode
  - Specific configurations could cause WiNG to crash when in the DIAG prompt mode
  - A memory leak in Cfgd was fixed in release 5.8.3 that resolves this issue
- Other Security Vulnerabilities
  - See Vulnerability Summary

These items are all addressed in the WiNG firmware update described below.

Effectivity Date

Kontron will implement the WiNG firmware update by **9/17/2018**.
Any products shipping on or after this date will have the new firmware version.

This update will change the top level revision of the product. This revision is indicated on the outside product label.

Product Revision	WiNG Firmware Version
Rev F	AP7532-5.8.2.0-030R
Rev G	AP7532-5.9.2.1-009R

Any units returned for repair that are at Rev F or below will be updated to Firmware AP7532-5.9.2.1-009R under MOD2.

Firmware Validation

Kontron has tested and performed regression testing with this release to confirm fixes to known issues and verify no impact to known avionics IFE configurations.

Updating the Firmware

Kontron will make available (upon request) the WiNG Firmware AP7532-5.9.2.1-009R and MIBs. It is recommended that you install and test this firmware version with your A100 units in the lab. It is also recommended that the A100 units on aircraft are updated. Please reference A100 User Guide (PN:

73001011-101_UG) Rev_A3 Section 6.5 for how to update the Firmware version, including how to remotely update on aircraft.

Returns/Repairs

Any systems returned for repair or replacement under warranty and/or paid for repair will be updated to this latest WiNG firmware starting on the Effectivity Date.

Additional Information

KRACK, WPA2 Protocol Flaw

General Vulnerability Summary:

A research paper titled “Key Installation Attacks: Forcing Nonce Reuse in WPAv2” published on October 16, 2017, identifies a weakness in WPAv2 which can allow a sophisticated attacker to decrypt the contents of messages exchanged between the client and the access point. Both WPAv2-PSK and WPAv2-Enterprise are affected. The vulnerability concerns the mechanisms for key exchange including key derivation, installation, and retransmission between APs and clients. The vulnerability allows a skilled attacker, albeit requiring significant expertise and computing power, within proximity of the wireless link to replay packets from a client and eventually decrypt the communication.

Additional details of the vulnerability can be found here: https://www.krackattacks.com/

Impact Details:
A majority of the vulnerability releases are addressed to WiFi clients rather than access points, with the exception of the ones relating to 802.11r (Fast Transition Roaming). Two main functional scenarios are currently under assessment for potential exposure:

1. AP as authenticator
   AP operates as authenticator for all WPA2 operations between clients and AP on WPAv2 protected SSIDs (PSK or EAP) and in support of 802.11r (Fast Roaming).
2. AP as client
   APs can operate as clients to other APs in support of WDS/Mesh. When operating as a client the AP could be vulnerable to message replaying in assuming they’re part of a retransmission.

Kontron A100 Product Impact:
The Cab-n-Connect Products has 802.11r (Fast bss transitions) and Group Key Rotation disabled by default. If you have enabled these features in your startup configuration, then this should be disabled. The firmware update removes the ability to enable this feature and disables this feature.

IOActive Research Paper

General Vulnerability Summary:
A research paper written by IOActive, identifies a weakness in the ExtremeWireless WiNG operating system that under certain conditions can create denial of service or elevated privilege conditions on the WiNG Access Point. To exploit these vulnerabilities, an attacker requires physical and/or LAN connectivity to the Access Point and/or the Wireless Controller, and it is noted that none of the vulnerabilities can be directly exploited over the air.

Impact Details:
This vulnerability notice includes advisories on vulnerability disclosures on the following software components within the ExtremeWireless WiNG operating system:

- RIM (Radio Interface Module) process
- MINT (Medium Independent Tunneling) Protocol
- Web User Interface

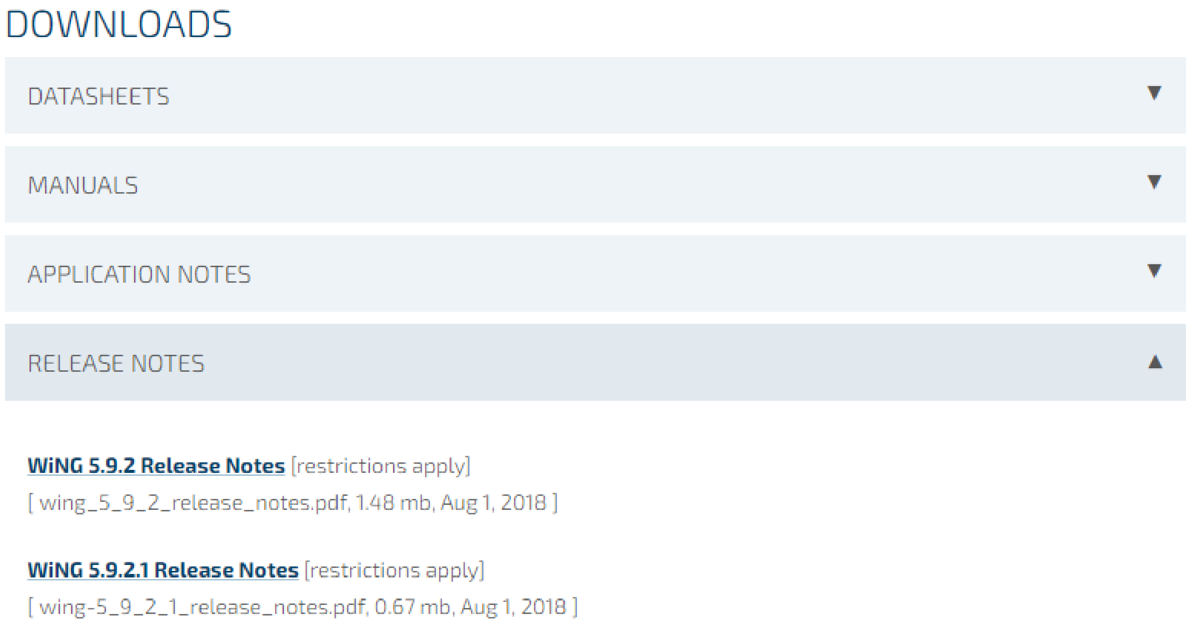
Kontron A100 Product Impact:
The security vulnerabilities described are not possible “Over-the-Air”.
When installed on the aircraft, an attacker will not have wired access to the Cab-n-Connect Products and the exploited use cases described are not typical configurations used on the aircraft.

Firmware version 5.9.1.3, and all subsequent releases, fixes these security vulnerabilities.

Additional details on these vulnerability and detailed use cases / responses are provided in the Vulnerability Notice from ExtremeWireless:
https://gtacknowledge.extremenetworks.com/articles/Vulnerability_Notice/VN-2018-003

Further Information

Additional information including the latest A100 User Guide, WiNG 5 Best Practices and User Guides, Application Notes and WiNG 5.9.2 / .1 Release Notes can be found on the Kontron A100 product page:
https://www.kontron.com/products/systems/aircraft-computers/servers/cab-n-connect-tm-a100.html



DOWNLOADS

DATASHEETS ▼

MANUALS ▼

APPLICATION NOTES ▼

RELEASE NOTES ▲

WiNG 5.9.2 Release Notes [restrictions apply]
[wing_5_9_2_release_notes.pdf, 1.48 mb, Aug 1, 2018]

WiNG 5.9.2.1 Release Notes [restrictions apply]
[wing-5_9_2_1_release_notes.pdf, 0.67 mb, Aug 1, 2018]

If you require further information of this planned update, please contact your sales person to review this further. Kontron is committed to supporting your program and working with you through this process. No response from customers will be deemed as acceptance of the planned update.

▶ CONTACT INFORMATION

RJ McLaren

rj.mclaren@us.kontron.com

Product Manager