Firmware for AWK-3131A-RCC Series Release Notes

Version: v1.2	Build: N/A
Release Date: Sep 30, 2020	

Applicable Products

N/A

Supported Operating Systems

N/A

New Features

• Added support for IEC 62443-4-2 functionality.
• The Network Status screen now shows the LLDP, ARP, and Bridge tables.
• Added support for the LLDP SNMP MIB.
• Added an option to add password encryption when exporting configuration files.
• Added support for DHCP client v2.
• Added support for wireless port mirroring.
• Added support for Wi-Fi remote connection check.

Enhancements

• Updated OpenSSL to version 1.1.0e.
• Changed the maximum clients for the DHCP server to 128.
• Increased the maximum length of user passwords to 32 characters.
• Increased the number of MAC/IP/Port filter entries to 32.

Bugs Fixed

Security
• The Wireless Search Utility cannot find clients that use the 4th WEP key.
• CVE-2018-10698: TELNET is enabled by default.
• CVE-2018-10690: HTTP is enabled and HTTPS is disabled by default.
• CVE-2018-10692: The session cookie does not have an HttpOnly flag.
• CVE-2018-10695: The "send email to admin account" function can be used to execute Linux commands on the device.
• CVE-2019-5136: Improper system access as a higher privilege user; an attacker can send commands while authenticated as a low privilege user to trigger this vulnerability.
• CVE-2019-5137: Exploitable Hard-coded Cryptographic Key allows for the decryption of captured traffic.
• CVE-2019-5138/CVE-2019-5140/CVE-2019-5141/CVE-2019-5142: Improper Neutralization of Special Elements used in an OS Command.
• CVE-2019-5139: Exploitable hard-coded credentials.
• CVE-2019-5143: Buffer Copy without Checking Size of Inpup may cause remote code execution.
• CVE-2019-5148: An attacker can send a crafted packet to execute a denial-of-service attack on the device.
• CVE-2019-5153: Stack-based Buffer Overflow.
• CVE-2019-5162: Improper remote shell access to the device; an attacker can send commands while authenticated as a low privilege user to trigger this vulnerability.
• CVE-2019-5165: An exploitable authentication bypass vulnerability; an attacker can trigger an authentication bypass by using a specially configured device hostname.

Web
• Specifying the maximum byte size of the primary RADIUS shared key will change the setting of the

secondary RADIUS server IP.
• Users are unable to configure RSTP settings when the device is in ACC operation mode.

DHCP
• Users are unable to set the number of DHCP server users to more than 128.

Function
• The ACC connection may sometimes fail when the ACC master power input status changes.

Changes

• Changed the default system description to the device model name.

Notes

N/A

Version: v1.0	Build: Build 18041016
Release Date: Jan 10, 2019	

Applicable Products

AWK-3131A-M12-RCC

Supported Operating Systems

N/A

New Features

First release

Enhancements

N/A

Bugs Fixed

N/A

Changes

N/A

Notes

N/A