Firmware for AWK-1137C Series Release Notes

Version: v1.5	Build: 20071510
Release Date: Jun 30, 2020	

Applicable Products

AWK-1137C series

Supported Operating Systems

N/A

New Features

• Added 8 channels (total 11) for Client-based Turbo Roaming channel scanning.
• Added support for Turbo Roaming in Slave Mode.
• Added support for AeroMag in Client-Router Mode.
• Added support for Wi-Fi Remote Connection Check.
• The WAN/LAN interface can now be set in Client-Router Mode.
• Added Indoor/outdoor channel list option.
• Added support for static Mac Clone.
• Added the Mirror Port feature.
• Added support for Management Frame Encryption.
• Added a progress bar to show the progress of firmware upgrades.
• Added an option to lock a user account when entering an invalid password.
• The system will record a system log if the device IP is changed via the Wireless Search Utility.
• Added support for Yahoo and Google email servers.
• Email messages now include device information.
• Added a function to gather additional Wi-Fi related information.
• Added an option to allow the use of special characters.
• Added support for Remote Diagnostics for engineer support.
• Added an option to show the PSK password in clear text.
• Added client isolation in AP mode.

Enhancements

[WLAN]
• When in Client Mode, the AWK now takes less time to reconnect after being disconnected by the AP.
• When in Client Mode, the AWK now takes less time to reconnect if MAC Clone is enabled.
• When in Client Mode, the AWK now takes less time to reconnect if the second EAPOL packet is lost.
• When in Client Mode, the AWK now takes less time to reconnect when plugging in Ethernet when the WLAN is establishing a connection.

Bugs Fixed

[WLAN]
• The AP responds to unicast probe requests, even if the AP is not the receiver.
• The GARP reply sent by the AP/Client does not have a VLAN tag.
• Unable to establish a Wi-Fi connection with APs that support 802.11r.
• G-mode-only clients are unable to associate with the AP.
• Authentication may fail when the client's security is set to Enterprise mode.
• The BSS node is cleaned in Master mode.
• The AWK does not connect to the AP with the strongest signal when there is no AP that satisfies the RSSI > keep alive threshold.

[Security]
• The Wireless Search Utility cannot find clients that use the 4th WEP key.
• CVE-2018-10694: The open "wireless interface" is enabled by default which can be exploited by unauthorized users.
• 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 and cause denial-of-service of 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 authentication bypass on specially configured device.

[Serial]
• The serial interface crashes when refreshing the serial status frequently.
• The inactivity timeout of serial port does not work accurately if the TCP alive check interval is less than 15 minutes.
• If one of the connections drops, it will not buffer and resend after the connection is restored.
• The serial connection drops when the DHCP IP is changed.
• DTR and RST do not restore to their initial state after timing out.

[WEB]
• Specifying the max byte size of the primary RADIUS shared key will change the setting of the secondary RADIUS server IP.
• Unable to set VAP3 to VAP9 as the RF-type for A/N Mixed mode, Channel 36, and channel width

20/40 MHz.
• Wi-Fi channel selection does not work properly on Quick Setup.
• The web server crashes when reading invalid content.
• Unable to import configuration after changing the device IP.

[Web]
• The number of DHCP server users cannot be set to more than 128.
• The DHCP server does not work properly when AeroMag AP enabled.

[MAC Clone]
• The client is unable to restore its original MAC address when unplugged from the LAN after disconnecting from the AP.

[AeroMag]
• Clients fail to initialize the configuration received from the AP.
• The WLAN LED turns off when renewing configuration settings or refreshing channels.
• Resetting to default settings does not clean configuration file.
• The Client page is blank during Quick Setup.
• Unable to configure AeroMag after performing channel analysis.

[Firewall]
• IP filter does not drop packets if MAC filter is disabled.
• Ports of device services such as the DHCP server are added to the white list automatically when port filtering is enabled.

[SNMP]
• SNMPv3 is unreachable after rebooting.
• SNMP sometimes causes a memory leak.

[MXview]
• Unable to import or export configuration and upgrade FW via MXview.

Changes

[WLAN]
• Changed the default multicast rate value.
• Changed the fix rate list according to the selected RF type.
• Changed the management frame rate according to the selected RF type.

• Changed the number of management frame transmission retries from 8 to 4.
• Changed the basic rate of G-only mode to be same rate as 802.11b.

[Security]
• CVE-2018-10694: The open "wireless interface" is now disabled by default.

[Firewall]
• Increased MAC/IP/Port filter entries up to 60.
• Changed the default rule policy to ACCEPT.

[WEB]
• Changed the default system description to the model name.
• Changed the web configuration import buffer size from 64K to 128K.
• User-level accounts can now no longer see other user account information.

Notes

This firmware version is currently incompatible with the officially released versions of Wireless Search Utility v2.6, MXConfig v2.6, and MXview v3.1. These utilities are expected to be updated to support this firmware version in Q4 2020. For urgent cases that require these utilities to be used with this firmware, please contact MOXA technical support for access to the beta version of these

Version: v1.3	Build: Build_18121212
Release Date: Dec 26, 2018	

Applicable Products

AWK-1137C-EU-T, AWK-1137C-JP-T, AWK-1137C-JP, AWK-1137C-US, AWK-1137C-EU, AWK-1137C-US-T

Supported Operating Systems

N/A

New Features

- IEC 62443-4-2 support
- 3rd SNMP trap server
- Web certificate support

Enhancements

N/A

Bugs Fixed

- Abnormal roaming handoff time if MAC clone is enabled
- Device reboot if it receives an abnormal beacon, which does not follow the IEEE standards.
- Issue with the error handler for abnormal Wi-Fi packets
- In the client-router mode, if an AP disappears from the network for a long period, an AWK-1137C client will not be able to reconnect to it.
- Static route of WLAN iface does not work for DHCP client in Client-Router mode

Changes

N/A

Notes

N/A

Version: v1.2	Build: Build_18020610
Release Date: Mar 23, 2018	

Applicable Products

AWK-1137C-JP, AWK-1137C-EU, AWK-1137C-US, AWK-1137C-EU-T, AWK-1137C-US-T, AWK-1137C-JP-T

Supported Operating Systems

N/A

New Features

N/A

Enhancements

N/A

Bugs Fixed

• Fixed CVE-2017-14459.

Changes

• Changed the format of the device name field to AWK-1137C_[the last six digits of the MAC address].
• Displays complete S/N information.

Notes

N/A

Version: v1.1	Build: Build_17102616
Release Date: N/A	

Applicable Products

AWK-1137C-EU, AWK-1137C-US, AWK-1137C-JP, AWK-1137C-EU-T, AWK-1137C-US-T, AWK-1137C-JP-T

Supported Operating Systems

N/A

New Features

N/A

Enhancements

N/A

Bugs Fixed

- The following CVE's are fixed: CVE-2017-13077, CVE-2017-13078, and CVE-2017-13080.

Changes

N/A

Notes

N/A

Version: v1.0	Build: Build 17080416
Release Date: N/A	

Applicable Products

AWK-1137C-EU, AWK-1137C-US, AWK-1137C-JP, AWK-1137C-EU-T, AWK-1137C-US-T, AWK-1137C-JP-T

Supported Operating Systems

N/A

New Features

• First release.

Enhancements

N/A

Bugs Fixed

N/A

Changes

N/A

Notes

N/A