Release Notes

Firmware 6.4.1

Advantech Czech s.r.o., Sokolska 71, 562 04 Usti nad Orlici, Czech Republic
This document was issued on 27th March, 2024.

Abstract

This document encompasses the following key sections:

- **Firmware Update Instructions:** Guides users through the firmware update process, ensuring a smooth and successful experience.
- **Description of New Features, Fixes, and Changes:** Provides detailed information about new features, enhancements, fixes for previous issues, and other significant changes included in the firmware update.
- **Known Issues Related to the Firmware Version:** Informs users about any existing issues or limitations with this firmware version, aiding in informed decision-making and preparation.

Firmware Release Information

- **Version**: 6.4.1
- **Release Date**: March 27, 2024
-  **Compatibility and Distribution**:

  Due to significant changes introduced in 6.4.0 update, extensive testing of the new firmware is strongly advised prior to its deployment in operational environments, when upgrading from version 6.3.x.

  For comprehensive compatibility details and distribution guidelines, see the *Firmware Compatibility Chart* document published with the specific firmware version.

Firmware and Product Documentation Notice

- **Firmware Versions in New Routers:** Not all new Advantech routers are shipped with this latest firmware release due to specific carrier or regional certifications. Check the *Firmware Compatibility Chart* document for the latest firmware information for your router model.
- **Router Configuration Information:** The most recent and detailed configuration information is available in the *Configuration Manual* for your router model.
- **Accessing Documents and Applications:** Visit the *Engineering Portal* at *icr.advantech.com* for product-related documents, applications, and firmware updates.

Contents

Part I.

Firmware Update Instructions

General Update Instructions and Notices

HTTPS Certificates:

- Following the release of firmware version 5.3.5, the router's HTTPS certificate format has been updated to enhance security measures. It is crucial to recognize that routers produced prior to this firmware version will not have their HTTPS certificates automatically updated during the firmware upgrade process.
- For manual HTTPS certificate updates, remove the existing certificate files found at `/etc/certs/https*` on the router. This action should be performed through an SSH connection. The certificates will be automatically regenerated in the new format upon the next reboot of the router.

FirstNet Firmware Specific Notes

Note: The following notes are specific to *FirstNet* products (ICR-3241..**-1ND** and ICR-4461..**-1ND**) and apply starting from firmware version 6.3.2, unless indicated otherwise.

- **Administration User Account:** Access via the *root* user for web or SSH logins is disabled. Utilize the *admin* account instead. The router label contains a unique password.
- **Disabled User Scripts:** Scripts set up through the GUI are unsupported. Scripts will convert to a Router App in updates to firmware version 6.3.7 or later. Note: Scripts will be deleted when updating to firmware versions from 6.3.2 to 6.3.6.
- **Different Default Settings:** Default router settings have been changed to improve security, deviating from standard configurations.
- **No FTP Support:** FTP configuration is removed from the GUI.
- **No Telnet Support:** Telnet configuration is removed from the GUI.
- **WiFi Security:** Support for WEP, WPA1, and WPA2-TKIP security protocols is discontinued.
- **OpenVPN Security Level:** Security levels *0 - Weak* and *1 - Low* are not allowed.
- **HTTP Restrictions:** Only HTTPS access is allowed with a minimum of TLS version 1.2.
- **MTU Settings:** The default MTU is set to 1342 bytes.
- **SNMP Restrictions:** SNMP write access is disabled.
- ***FirstNet* Router App Changes:** Some functionalities previously in the *FirstNet* Router App are now embedded in the firmware, focusing the app on monitoring the security status of *FirstNet* routers.

Part II.

Description of New Features, Changes, and Fixes

Added

WiFi Module Information Display

Additional information regarding the WiFi module has been integrated into the *WiFi Status* page. This update furnishes details about the WiFi chip, firmware version, and supported modes for the module.

USB Port Disabling

An option to disable the external USB port on ICR-4400 platforms has been introduced to increase device security. This functionality is accessible by deselecting the *Enable external USB port* option located at the top of the *USB Port* configuration page. Note that on the ICR-4461-1N model, which holds FirstNet certification, the external USB port is inherently disabled.

`net-snmptrap` and `net-snmpinform` Commands

The firmware now includes `net-snmptrap` and `net-snmpinform` commands for sending SNMP v1/v2c/v3 notifications. These additions enhance the network management capabilities of our devices. Detailed usage instructions are available in the *Commands and Scripts* Application Note.

`less` Command Integration

The `less` command has been integrated into our firmware, improving the usability of reading large text files. Users can efficiently navigate through files screen by screen or page by page, with functionalities for scrolling, text searching, and direct line access. This significantly enhances file viewing and editing efficiency. For more details on using the `less` command, consult the *Commands and Scripts* Application Note.

System File Enhancement

The system identification file at `/etc/os-release` has been enhanced to include additional essential router identification information. New fields such as `ICR_PLATFORM`, `ICR_COUNTRY`, and `ICR_PRODUCT_OID` have been added to support Router Apps that utilize this information.

Firmware File Identification

A `.ver` file containing firmware version information has been added to the firmware `.bin` tar file to facilitate better identification of the firmware file.

Changed

Firmware Changelog Renamed and Reformatted

The firmware changelog file, previously named `version.txt` within the firmware distribution, is now `CHANGELOG.md`. This file has transitioned to a Markdown format, aligning with the *Keep a Changelog* guidelines, enhancing readability and structure.

DHCP Lease Time Flexibility Enhanced

The minimum allowable DHCP Lease Time in Ethernet and WiFi Access Point (AP) configurations has been lowered from 60 seconds to 5 seconds. This adjustment supports the integration of specific device types requiring shorter lease times. The internal DHCP client continues to accept a minimum lease time of 20 seconds.

`dnsmasq` Software Upgrade

The `dnsmasq` software has been upgraded to version 2.90. This version resolves the high-severity vulnerabilities identified as *CVE-2023-28450* and *CVE-2023-50387*, reinforcing our commitment to security. For detailed insights into this upgrade, please view the *dnsmasq changelog*.

`zlib` Library Update

The `zlib` library has been updated to version 1.3.1. This revision was prompted by *CVE-2023-45853* (critical), which, despite not impacting our product directly, was flagged by security scanners. This proactive update underscores our dedication to maintaining the highest security standards.

Fixed

Root Filesystem Space Optimization

We've reclaimed all unused space on the root filesystem after firmware upgrades on the ICR-4400 platform. Following the upgrade, we optimized the partition size, expanding it to its maximum possible value. Free space can also be manually reclaimed by executing the `resize2fs` command.

WPA3 Encryption Detection Improvement

We've addressed an issue in the WiFi scan results where WPA3 encryption was not consistently identified, ensuring accurate encryption detection.

DHCP Server File Creation Permissions

Filesystem permissions have been corrected to allow the DHCP server to appropriately create lease files.

Router Apps Online Installation Display Enhancement

Resolved an issue affecting the online installation of RouterApps, now correctly displaying more than 100 items.

Accurate Ethernet Port Detection for PPPoE

Fixed an error in PPPoE Interface configuration that led to devices with 2 Ethernet ports mistakenly presenting an option for 3 ports.

WiFi Scan Script Return Code Correction

Adjusted the return code of `/etc/init.d/wifi1 scan` scripts to ensure a single record is returned on failure, addressing occasional blank screens in the GUI during WiFi scanning.

WiFi STA IPv6 Configuration Dynamism

Corrected the enabling/disabling behavior of *IP Address* and *Subnet Mask / Prefix* in the configuration of WiFi STA IPv6, making it responsive to DHCP setting changes.

Part III.

Known Issues Related to the Firmware Version

Firmware Update – Unexpected Filename

There is a known issue that occurs if the filename of the firmware intended for your router has been altered. This can affect both manual firmware updates and the Automatic Update feature. When encountering this issue, the following warning message is displayed: *"You are trying to upload file 'xx.bin' but 'yy.bin' is expected. Are you sure to continue?"* To resolve this issue, please follow the instructions provided in Part I - Firmware Update Instructions of this document.

WiFi Configuration – Lost After Firmware Downgrade

Be aware that if you downgrade your firmware to a version earlier than 6.2.0, all existing WiFi configurations will be completely lost. It's important to back up your configuration before proceeding with such a downgrade.

ICR-3200 – Country Code for WiFi

In the initial firmware version for the ICR-3200 WiFi module, there is a limitation regarding the setting of the country code. Any modifications to the country code made on the configuration page will not have any effect. This is because the country code for the WiFi module is pre-set during the manufacturing process, based on the intended region of product distribution.

SmartStart SL302 – Cellular Network Authentication

For the SmartStart SL302 router equipped with the Telit LE910-NA1 cellular module firmware version 20.00.522, there is a known limitation: It is not possible to use a username and password for authentication when connecting to the Mobile WAN network. This restriction specifically affects settings configured on the *Mobile WAN Configuration* page.
To check the firmware version of your cellular module, visit the *Mobile WAN Status* page in the router's web GUI, where it is listed under the *Mobile Network Information* section.