Firmware 6.3.9

RELEASE NOTES

Abstract

This document describes:

- Firmware update instructions.
- Description of all new features, fixes, and other changes implemented in the firmware.
- Known issues related to a firmware version

Firmware Details

- **Firmware version**: 6.3.9
- **Release date**: January 4, 2023
- **Compatibility**: Advantech routers; see the Firmware Distribution Overview

Please note that not all new Advantech routers are produced and shipped with the latest release of the firmware. The reason for this is usually an existing certification valid for a specific carrier or a region. For more information about the latest version of the firmware for your router, see the *Firmware Distribution Overview* document.

For current and detailed information about the router configuration see the latest version of the Configuration Manual for your router.

Product-related documents and applications including the firmware can be obtained on *Engineering Portal* at icr.advantech.cz address.

Advantech Czech s.r.o., Sokolska 71, 562 04 Usti nad Orlici, Czech Republic
This document was issued on January 9, 2023

Part I

Firmware Update Instructions

General Update Instructions and Notices

HTTPS certificates: The HTTPS certificate format in the router was updated in FW 5.3.5 to improve the security. Existing HTTPS certificates on previously manufactured routers will not automatically be updated with the firmware update! It is possible to update the HTTPS certificates by deleting the files within `/etc/certs/https*` in the router (e.g. via SSH). The certificates will be re-created automatically during the router's next start.

Specific Update Instructions

New filename: If the firmware filename for your router was changed, as listed in Table 1, you will get an issue during the manual or automatic firmware update. The following warning message will appear: *You are trying to upload file "xx.bin" but "yy.bin" is expected. Are you sure to continue?*

To go ahead with the **manual** firmware update, check the table below for details about recent firmware filename changes and make sure you have the correct firmware file for your router. Now, you can confirm the displayed warning message.

To go ahead with the **automatic** firmware update, rename the new firmware file (*.bin and *.ver) to the filename valid before the filename change. This should allow the router to pass through the process of automatic firmware update. Next time, the automatic firmware update feature will work as expected with no need to rename the file.

Router model	FW ver.	New filename	Original filename
SmartMotion ST352 SmartMotion ST355	6.0.2	SPECTRE-v3T-LTE.bin	BIVIAS-v3LL.bin
SmartStart SL302	6.0.3	SPECTRE-v3L-LTE-US.bin	SPECTRE-v3L-LTE-AT.bin

Table 1: Recent Firmware Filename Changes

Updating Firmware Version Earlier than 5.3.0

It is necessary to follow specific update instructions below only if you are updating from firmware older than 5.3.0.

Due to a bug in the firewall (now fixed) when a WAN device is part of a bridged interface, caution should be taken when updating in the following case:

Condition:	When a WAN device is part of a bridged interface, access to that WAN device (HTTPS, SSH) is always granted regardless of configuration.
Problem:	If this is your configuration, it is highly likely that you are not aware of this, so the undesired effect of the bridge firewall fix may make the router inaccessible.
Recommended Action:	Enable access to both, the web and ssh services, before updating if you want to keep the current behavior (access to the WAN interface). This can be done on the *NAT* page in the *Configuration* section of the router's Web interface.

Change the root's password:

It is necessary to change the password of the *root* user when updating to the firmware version 5.3.0 or newer. The reason for this is an update of the authentication system (encryption algorithm *crypt* was changed to *MD5*; passwords are now stored in the `/etc/shadow` file instead of `/etc/passwd` file). The change of the password is required before setting up the remote access on the *NAT Configuration* page.

Please note that when downgrading from 5.3.0+ to an earlier firmware version, the password of the *root* user is reset to the default one, which is *root*.

FirstNet Firmware Specific Updates

Note: The changes described below are valid for *FirstNet* products (**ICR-3241-1ND** and **ICR-3241W-1ND**) only and have been made in firmware version 6.3.2 unless otherwise noted.

- **Administration User Account** – The *root* user is disabled for web or SSH logins. Use the *admin* user account instead. See the router label for a unique password.
- **Disabled User Scripts** – User scripts, which could have been configured in the GUI before, are not supported anymore. Existing scripts will be converted automatically to a Router App only during a firmware update to version 6.3.7 or higher. Note that user scripts will be deleted when the firmware is upgraded to versions 6.3.2 through 6.3.6.
- **Different Default Settings** – The router's default setting is different from the standard setting due to higher security requirements.
- **No FTP Support** – There is no FTP configuration in the GUI.
- **No Telnet Support** – There is no Telnet configuration in the GUI.
- **WiFi Security** – Configuration of WEP, WPA1, and WPA2-TKIP WiFi security protocols are not available.
- **HTTP Restrictions** – Only HTTPs access can be configured. The minimal configurable TLS (Transport Layer Security) is TLS 1.2.
- **MTU Settings** – The MTU (Maximum Transmission Unit) is configured to 1342 bytes.
- **SNMP Restrictions** – SNMP write access is disabled.
- ***FirstNet* Router App Changes** – Some features implemented in the *FirstNet* Router App are now supported by the router firmware. The *FirstNet* Router App is dedicated to reviewing the required security status of *FirstNet* routers.

Part II

Changelog

Legend: Affected products are marked as shown below for every changelog item:

Affected product | Not affected product

Fixed reading information about mobile connection via SNMP

SPECTRE 3G | SPECTRE RT | SPECTRE LTE-AT | SPECTRE LTE-VZ
ER75i v2 | UR5i v2 | XR5i v2 | LR77 v2 | CR10 v2 | UR5i v2L | RR75i v2 | LR77 v2L | XR5i v2E
Bivias v2HC | Bivias v2LC | Bivias v2LL | Bivias v2LH | Bivias v2HH
SmartFlex SR300 | SmartFlex SR303 | SmartFlex SR304 | SmartFlex SR305 | SmartFlex SR306 | SmartFlex SR307
SmartFlex SR308 | SmartFlex SR309 | SmartFlex SR310 | SmartStart SL302 | SmartStart SL304 | SmartStart SL305
SmartStart SL306 | SmartMotion ST352 | SmartMotion ST355 | ICR-320x | ICR-321x | ICR-323x | ICR-324x
ICR-203x | ICR-204x | ICR-241x | ICR-243x | ICR-244x | ICR-253x | ICR-263x | ICR-270x | ICR-273x | ICR-283x
ICR-383x | ICR-440x | ICR-443x | ICR-445x

We have fixed the reading of mobile SNMP entries. The issue has been recognized in firmware version 6.3.8. Please note that this issue may affect the mobile data reported in the *R-SeeNet* system.

Fixed occasional IPsec hang when terminating connection

SPECTRE 3G | SPECTRE RT | SPECTRE LTE-AT | SPECTRE LTE-VZ
ER75i v2 | UR5i v2 | XR5i v2 | LR77 v2 | CR10 v2 | UR5i v2L | RR75i v2 | LR77 v2L | XR5i v2E
Bivias v2HC | Bivias v2LC | Bivias v2LL | Bivias v2LH | Bivias v2HH
SmartFlex SR300 | SmartFlex SR303 | SmartFlex SR304 | SmartFlex SR305 | SmartFlex SR306 | SmartFlex SR307
SmartFlex SR308 | SmartFlex SR309 | SmartFlex SR310 | SmartStart SL302 | SmartStart SL304 | SmartStart SL305
SmartStart SL306 | SmartMotion ST352 | SmartMotion ST355 | ICR-320x | ICR-321x | ICR-323x | ICR-324x
ICR-203x | ICR-204x | ICR-241x | ICR-243x | ICR-244x | ICR-253x | ICR-263x | ICR-270x | ICR-273x | ICR-283x
ICR-383x | ICR-440x | ICR-443x | ICR-445x

We have fixed IPsec tunnel termination that sometimes failed and caused a reboot.

Improved security by running VRRP in unprivileged mode

SPECTRE 3G | SPECTRE RT | SPECTRE LTE-AT | SPECTRE LTE-VZ
ER75i v2 | UR5i v2 | XR5i v2 | LR77 v2 | CR10 v2 | UR5i v2L | RR75i v2 | LR77 v2L | XR5i v2E
Bivias v2HC | Bivias v2LC | Bivias v2LL | Bivias v2LH | Bivias v2HH
SmartFlex SR300 | SmartFlex SR303 | SmartFlex SR304 | SmartFlex SR305 | SmartFlex SR306 | SmartFlex SR307
SmartFlex SR308 | SmartFlex SR309 | SmartFlex SR310 | SmartStart SL302 | SmartStart SL304 | SmartStart SL305
SmartStart SL306 | SmartMotion ST352 | SmartMotion ST355 | ICR-320x | ICR-321x | ICR-323x | ICR-324x
ICR-203x | ICR-204x | ICR-241x | ICR-243x | ICR-244x | ICR-253x | ICR-263x | ICR-270x | ICR-273x | ICR-283x
ICR-383x | ICR-440x | ICR-443x | ICR-445x

The VRRP (Virtual Router Redundancy Protocol) service now runs in the unprivileged mode having restricted access to system resources. We have made this measure due to security reasons.

Fixed Linux Kernel Vulnerability

SPECTRE 3G | SPECTRE RT | SPECTRE LTE-AT | SPECTRE LTE-VZ
ER75i v2 | UR5i v2 | XR5i v2 | LR77 v2 | CR10 v2 | UR5i v2L | RR75i v2 | LR77 v2L | XR5i v2E
Bivias v2HC | Bivias v2LC | Bivias v2LL | Bivias v2LH | Bivias v2HH
SmartFlex SR300 | SmartFlex SR303 | SmartFlex SR304 | SmartFlex SR305 | SmartFlex SR306 | SmartFlex SR307
SmartFlex SR308 | SmartFlex SR309 | SmartFlex SR310 | SmartStart SL302 | SmartStart SL304 | SmartStart SL305
SmartStart SL306 | SmartMotion ST352 | SmartMotion ST355 | ICR-320x | ICR-321x | ICR-323x | ICR-324x
ICR-203x | ICR-204x | ICR-241x | ICR-243x | ICR-244x | ICR-253x | ICR-263x | ICR-270x | ICR-273x | ICR-283x
ICR-383x | ICR-440x | ICR-443x | ICR-445x

This update has fixed CVE-2022-45934 (high) security vulnerability in the Linux kernel.

Updated OpenSSL Library

SPECTRE 3G | SPECTRE RT | SPECTRE LTE-AT | SPECTRE LTE-VZ
ER75i v2 | UR5i v2 | XR5i v2 | LR77 v2 | CR10 v2 | UR5i v2L | RR75i v2 | LR77 v2L | XR5i v2E
Bivias v2HC | Bivias v2LC | Bivias v2LL | Bivias v2LH | Bivias v2HH
SmartFlex SR300 | SmartFlex SR303 | SmartFlex SR304 | SmartFlex SR305 | SmartFlex SR306 | SmartFlex SR307
SmartFlex SR308 | SmartFlex SR309 | SmartFlex SR310 | SmartStart SL302 | SmartStart SL304 | SmartStart SL305
SmartStart SL306 | SmartMotion ST352 | SmartMotion ST355 | ICR-320x | ICR-321x | ICR-323x | ICR-324x
ICR-203x | ICR-204x | ICR-241x | ICR-243x | ICR-244x | ICR-253x | ICR-263x | ICR-270x | ICR-273x | ICR-283x
ICR-383x | ICR-440x | ICR-443x | ICR-445x

We have updated the OpenSSL library to version 1.1.1s. For more details about this release, see the OpenSSL Changes webpage.

Updated BusyBox Software

SPECTRE 3G | SPECTRE RT | SPECTRE LTE-AT | SPECTRE LTE-VZ
ER75i v2 | UR5i v2 | XR5i v2 | LR77 v2 | CR10 v2 | UR5i v2L | RR75i v2 | LR77 v2L | XR5i v2E
Bivias v2HC | Bivias v2LC | Bivias v2LL | Bivias v2LH | Bivias v2HH
SmartFlex SR300 | SmartFlex SR303 | SmartFlex SR304 | SmartFlex SR305 | SmartFlex SR306 | SmartFlex SR307
SmartFlex SR308 | SmartFlex SR309 | SmartFlex SR310 | SmartStart SL302 | SmartStart SL304 | SmartStart SL305
SmartStart SL306 | SmartMotion ST352 | SmartMotion ST355 | ICR-320x | ICR-321x | ICR-323x | ICR-324x
ICR-203x | ICR-204x | ICR-241x | ICR-243x | ICR-244x | ICR-253x | ICR-263x | ICR-270x | ICR-273x | ICR-283x
ICR-383x | ICR-440x | ICR-443x | ICR-445x

This update has fixed CVE-2022-30065 (high) security vulnerability in the *BusyBox* software.

Updated Net-SNMP Software

SPECTRE 3G | SPECTRE RT | SPECTRE LTE-AT | SPECTRE LTE-VZ
ER75i v2 | UR5i v2 | XR5i v2 | LR77 v2 | CR10 v2 | UR5i v2L | RR75i v2 | LR77 v2L | XR5i v2E
Bivias v2HC | Bivias v2LC | Bivias v2LL | Bivias v2LH | Bivias v2HH
SmartFlex SR300 | SmartFlex SR303 | SmartFlex SR304 | SmartFlex SR305 | SmartFlex SR306 | SmartFlex SR307
SmartFlex SR308 | SmartFlex SR309 | SmartFlex SR310 | SmartStart SL302 | SmartStart SL304 | SmartStart SL305
SmartStart SL306 | SmartMotion ST352 | SmartMotion ST355 | ICR-320x | ICR-321x | ICR-323x | ICR-324x
ICR-203x | ICR-204x | ICR-241x | ICR-243x | ICR-244x | ICR-253x | ICR-263x | ICR-270x | ICR-273x | ICR-283x
ICR-383x | ICR-440x | ICR-443x | ICR-445x

This update has fixed the Net-SNMP software security issues; see CVE-2022-44792 (medium) and CVE-2022-44793 (medium) for details.

Part III

Known Issues

Firmware Update – Unexpected Filename

If the filename of firmware for your router was changed, you could have an issue during manual firmware update or with Automatic Update feature. This warning message will appear: *"You are trying to upload file "xx.bin" but "yy.bin" is expected. Are you sure to continue?"* To fix this issue follow instructions in Part I - Firmware Update Instructions.

Automatic Update – Update to Version 6.1.10

The feature of automatic firmware update will not recognize the firmware version 6.1.10 as a new version in case the installed version of firmware is from 6.1.0 to 6.1.8. To fix this issue, either update the firmware by the automatic update to version 6.1.9 first or update it manually directly to the version 6.1.10.

WiFi Configuration – Lost After Firmware Downgrade

If the firmware is downgraded to the version earlier than 6.2.0, the WiFi configuration will be lost completely.

ICR-3200 – Country Code for WiFi

The first version of the firmware for the WiFi module does not support the settings of the country code. Due to this issue, the settings of the country code made on the configuration page has no effect at all. The country code is set up during the manufacturing process according to the product destination region.

SmartStart – Cellular Network Registration

It is necessary to use router's firmware version 6.1.5 or higher if the *Telit* cellular module installed in your SmartStart router has following version of the firmware:

- *Telit LE910-EU V2* cellular module with firmware version 20.00.403 or newer,
- *Telit LE910-NA1* cellular module with firmware version 20.00.014 or newer.

Note: The model name and firmware version of the cellular module can be found on router's web GUI at *Mobile WAN Status* page in *Mobile Network Information* section.

SmartStart SL302 – Cellular Network Authentication

It is not possible to use username and password when connecting to Mobile WAN network (on *Mobile WAN Configuration* page) if your SmartStart SL302 router has the 20.00.522 firmware version inside the Telit LE910-NA1 cellular module. The version of cellular module firmware can be found at *Mobile WAN Status* page in *Mobile Network Information* section.

SmartStart SL302 – SMS in *Verizon* Network

SmartStart SL302 router (equipped with the *Telit* modules *LE910-SV1* or *LE910-NA1*) supports sending and receiving of SMS in *Verizon* cellular network since the firmware version 6.1.4. Please note that to support SMS receiving, cellular module with *Verizon* firmware version higher than 20.00.012 is required.

Incorrect Mobile Data

The mobile interface data read by the SNMP or reported by the *R-SeeNet* system may be incorrect for router firmware version 6.3.8. Please update the firmware to a higher version to fix this issue.