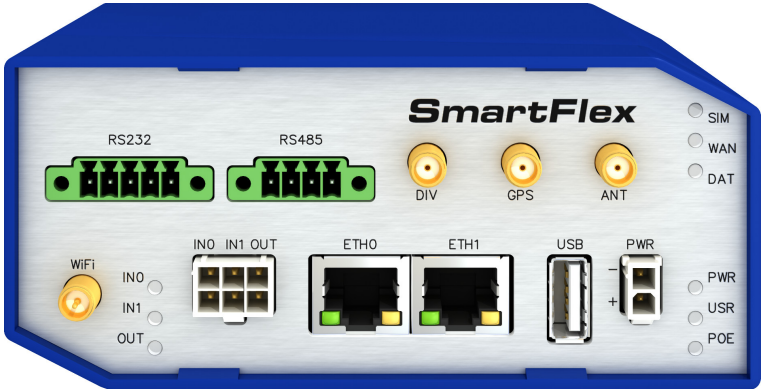




# Firmware 6.3.3

## 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:** 6.3.3
- **Release date:** December 13, 2021
- **Hardware compatibility:** applicable to the Advantech routers

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](http://icr.advantech.cz) address.

# **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*.

# **Part II**

# **Changelog**



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

Affected product    Not affected product

## WireGuard VPN Support

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-243x ICR-253x ICR-383x ICR-443x ICR-445x

*WireGuard* is a communication protocol and free open-source software that implements encrypted virtual private networks (VPNs) and is designed with the goals of ease usage, high-speed performance, and low attack surface. It aims for better performance and more power than IPsec and OpenVPN, two common tunneling protocols. The WireGuard protocol passes traffic over UDP. Advantech routers now support up to four WireGuard tunnel configurations. For more information, see the [Configuration Manual](#) of your router.

## Cisco FlexVPN Support

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-243x ICR-253x ICR-383x ICR-443x ICR-445x

We have added support for the *Cisco FlexVPN*. Internet Key Exchange Version 2 (IKEv2), a next-generation key management protocol based on RFC 4306, is an enhancement of the IKE Protocol. IKEv2 is used for performing mutual authentication and establishing and maintaining security associations (SAs). FlexVPN is Cisco's implementation of the IKEv2 standard featuring a unified paradigm and CLI that combines site-to-site, remote access, hub-and-spoke topologies and partial meshes (spoke to spoke direct). FlexVPN offers a simple but modular framework that extensively uses the tunnel interface paradigm while remaining compatible with legacy VPN implementations using crypto maps. To enable the Cisco FlexVPN feature, enable the *Cisco FlexVPN* on the *IPSec* configuration page.

## Signal Strength Indication Improvement

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-243x	ICR-253x	ICR-383x	ICR-443x	ICR-445x			

Cellular signal strength, reported on the *Mobile WAN* status page, was enhanced with a new field for *SINR* value. This parameter is available in the SNMP mobile subtree as well.

## RST Button Wakeup

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-243x	ICR-253x	ICR-383x	ICR-443x	ICR-445x			

A new feature, waking up from the low power mode by pressing the *RST* (reset) button, is now available.

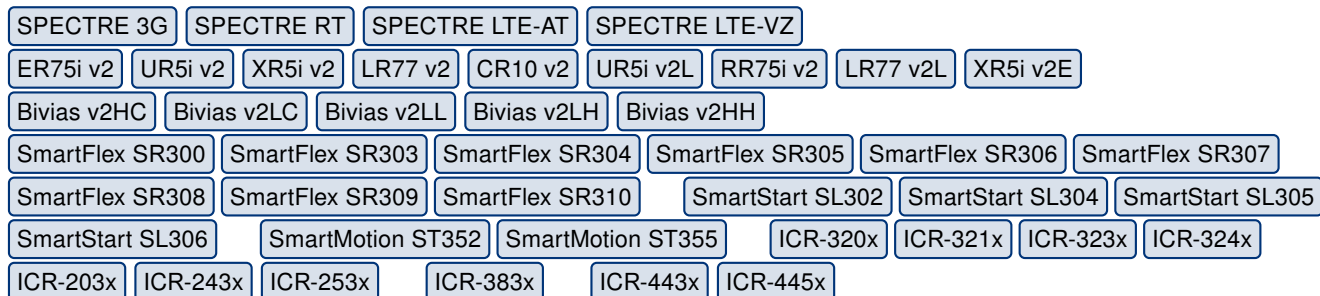
## Changed RST Button Behavior

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-243x	ICR-253x	ICR-383x	ICR-443x	ICR-445x			

For the router's factory reset, when the *RST* button is held for more than four seconds, the reset is performed when the button is released. Originally, the reset was performed four seconds after the button was pressed.

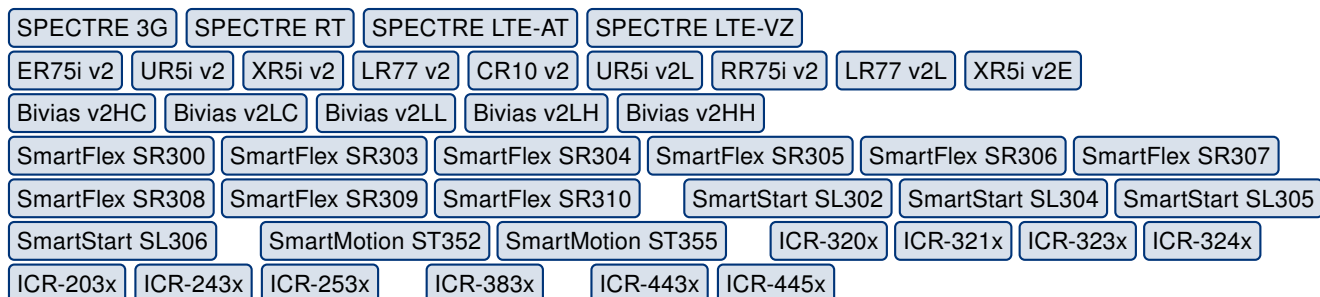


## LAN GUI Menu Renamed



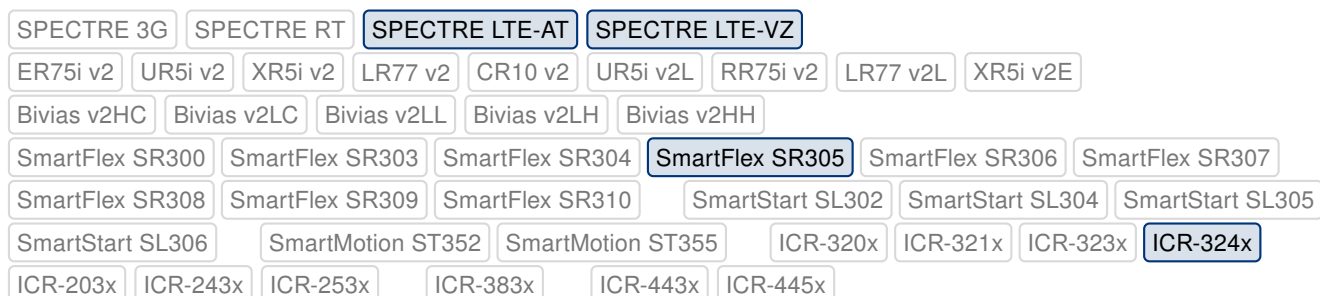
We have changed the name for the Ethernet interfaces in the GUI. The menu item changed from *LAN* to *Ethernet* and the sub-menus from *Primary LAN* to *ETH0*, *Secondary LAN* to *ETH1*, etc.

## Location and Name in GUI



*Location* and *Name* are now always visible in the top right corner of the GUI, not only when configured. If not configured, the "N/A" text is displayed here instead. You can enter both these entries in the *Services* -> *SNMP* configuration menu.

## Enabled MTU Discovery



We have enabled the automatic MTU discovery feature for the cellular network, which may decrease the MTU value. This update will fix a communication issue in networks not supporting the default MTU 1500 bytes.

## Changed GRE TTL

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-243x	ICR-253x	ICR-383x	ICR-443x	ICR-445x			

The TTL for the GRE packet was set to a fixed value of 64 bytes. This solution will prevent issues with the GRE tunnel in some specific scenarios.

## Fixed IPsec Issue

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-243x	ICR-253x	ICR-383x	ICR-443x	ICR-445x			

We have fixed the issue for route-based IPsec. If the responder's remote IP address was within the remote subnet, the router lost remote access to the device via (M)WAN.

## Fixed SIM PIN Issue

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-243x	ICR-253x	ICR-383x	ICR-443x	ICR-445x			

This issue caused the affected cellular module not to accept the SIM PIN.

### Fixed Possible XSS Attack

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-243x	ICR-253x	ICR-383x	ICR-443x	ICR-445x			

We have fixed the possible reflected XSS attack when a malicious code could be executed in the web browser. The router itself is not affected by this vulnerability.

### A Fix for snmptrap Program

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-243x	ICR-253x	ICR-383x	ICR-443x	ICR-445x			

We have fixed the snmptrap program to exit with code 1 if sending an SNMP has failed.

### Fixed Kernel Compatibilities

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-243x	ICR-253x	ICR-383x	ICR-443x	ICR-445x			

We have fixed an external kernel modules compatibility issue. This issue was observed in the firmware version 6.3.2 and may cause a crash when starting some kernel modules during the router's startup.

### Fixed USB and DMA Drivers Issues

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-243x	ICR-253x	ICR-383x	ICR-443x	ICR-445x			

We have fixed several USB and DMA drivers issues by backporting the fixes from the kernel version 4.14.250.

### Fixed I<sup>2</sup>C Driver Issues

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-243x	ICR-253x	ICR-383x	ICR-443x	ICR-445x			

We have fixed several I<sup>2</sup>C driver issues. These issues may get the router into a state when it cannot start up at all.

### Upgraded WiFi Module Firmware

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-243x	ICR-253x	ICR-383x	ICR-443x	ICR-445x			

The WiFi module firmware was upgraded to version 8.9.0.0.88. This update has fixed [CVE-2020-24588](#) (low), [CVE-2020-26146](#) (medium), [CVE-2020-26140](#) (medium) and [CVE-2020-26143](#) (medium).

## Upgraded 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-243x	ICR-253x	ICR-383x	ICR-443x	ICR-445x			

The *BusyBox* software suite was upgraded from version 1.29.3 to version 1.34.1. Many changes, including many security fixes, have been made, see the webpage at <https://busybox.net/news.html>.

## Updated OpenSSH 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-243x	ICR-253x	ICR-383x	ICR-443x	ICR-445x			

We have updated the *OpenSSH* software to version 8.8p1. This update has fixed [CVE-2016-20012](#) (medium) and [CVE-2021-41617](#) (high). For more details about this release, see the webpage at <https://www.openssh.com/releases.html>.

## Updated strongSwan 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-243x	ICR-253x	ICR-383x	ICR-443x	ICR-445x			

We have updated the *strongSwan* software to version 5.9.4. This update has fixed [CVE-2021-41990](#) (high) and [CVE-2021-41991](#) (high). For more details about this release, see the webpage at <https://github.com/strongswan/strongswan/releases/tag/5.9.4>.

## **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.