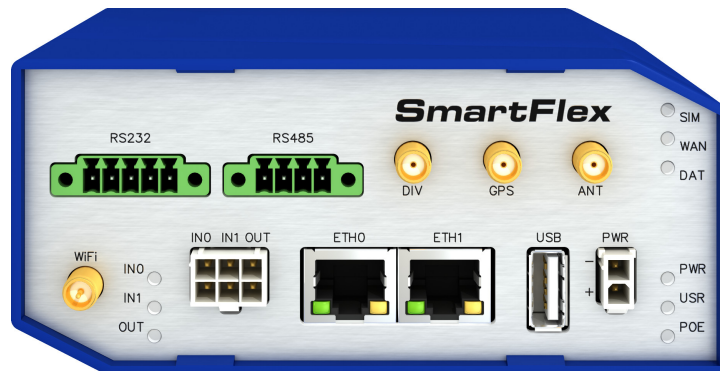


Firmware 6.1.8

RELEASE NOTES



ADVANTECH

Abstract

This document describes:

- Firmware upgrade instructions.
- Description of all new features, fixes and other changes implemented in firmware 6.1.8.
- Known issues.

For detailed information about firmware 6.1.8, see the Configuration Manual for your router.

Firmware Details

- **Version:** 6.1.8
- **Release date:** November 8, 2018
- **Hardware compatibility:** This firmware is applicable to any router made by Advantech B+B SmartWorx s.r.o.



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

Part I

Firmware Upgrade Instructions

General Upgrade Instructions and Notices

HTTPS certificates: The HTTPS certificate creation in the router was updated in FW 5.3.5 in order to improve security. Existing HTTPS certificates on previously manufactured routers will not automatically be upgraded with the firmware upgrade! It is possible to upgrade 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.



Python user module is not uploaded by default to the produced routers with firmware of version 6.0.2 and later. Python user module can be downloaded from [Engineering Portal](#) on [this link](#).



The **SPECTRE v3 LTE** and **SPECTRE v3 ERT** routers were renamed to **SmartFlex**. You will find them under this name in the Changelog below.

Specific Upgrade Instructions – new filename

If the filename of a firmware for your router was changed recently, then you can have an issue during manual firmware updating or with automatic firmware update feature. Following warning message will appear during the firmware updating process: *"You are trying to upload file "xx.bin" but "yy.bin" is expected. Are you sure to continue?"*

To proceed with the firmware updating please follow these steps: Check the table below with details of recent firmware filename changes for routers and make sure you have the correct firmware file for your router. Go ahead with manual firmware updating and confirm displayed warning message.

To proceed with automatic firmware updating, rename new firmware files (*.bin and *.ver) to filenames valid before the filename change. This should allow the router to pass through the process of automatic firmware updating. Next time, the automatic firmware update feature will work as expected and no other file renaming will be required.

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

Specific Instructions for Upgrading from Firmware Older than 5.3.0



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

Due to a (now fixed) bug in the firewall when a WAN device is part of a bridged interface, caution should be taken when upgrading in 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 render the router inaccessible.
- Recommended Action:** Enable access to both the web and ssh services before upgrading if you want to retain 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.

Changing the password

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

Please note that when downgrade from 5.3.0+ to previous firmware versions, the password for user *root* is reset to default ("root").

Part II
Changelog



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

Affected router version Router version not affected

Added *sync* command

ER75i 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 SmartStart SL302 SmartStart SL304 SmartMotion ST352 SmartMotion ST355

The *sync* command is supported by the firmware from now. This command forces an immediate transfer of buffered data blocks in memory or in FILES to the disk.

Synopsis:

`sync [OPTIONS] [FILES]...`

Options:

Option	Description
-d	Avoid syncing metadata.
-f	Sync filesystems underlying FILES.

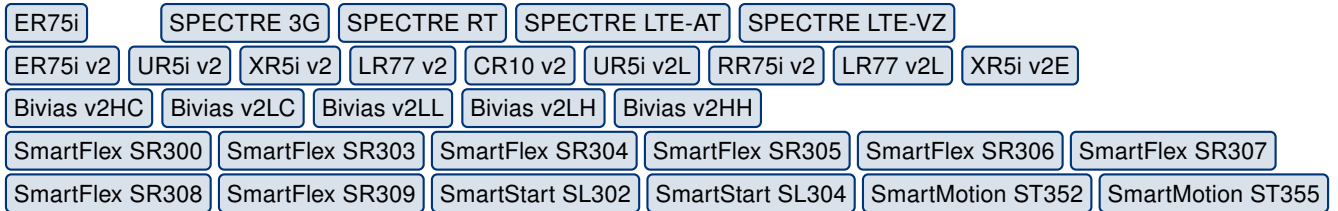
Table 2: sync options

Added configuration of *Syslog* service

ER75i 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 SmartStart SL302 SmartStart SL304 SmartMotion ST352 SmartMotion ST355

New configuration page *Configuration/Services/Syslog* was added to the GUI for configuration of *Syslog* service. On this page, the size of syslog can be restricted by specification of maximal number of log rows. Optionally, the IP address and UDP port can be configured for the real-time syslog distribution.

Added logging of user actions



New actions are from now logged into the System Log. These actions are listed below:

- A user has logged in to the router’s web GUI.
- A user has logged out from the router’s web GUI.
- The *Apply* button was pressed (except configuration of user modules).
- A user module was installed on the router.
- A user module was removed from the router.

An example of the System Log, with the new actions logged, is shown on the Figure below.

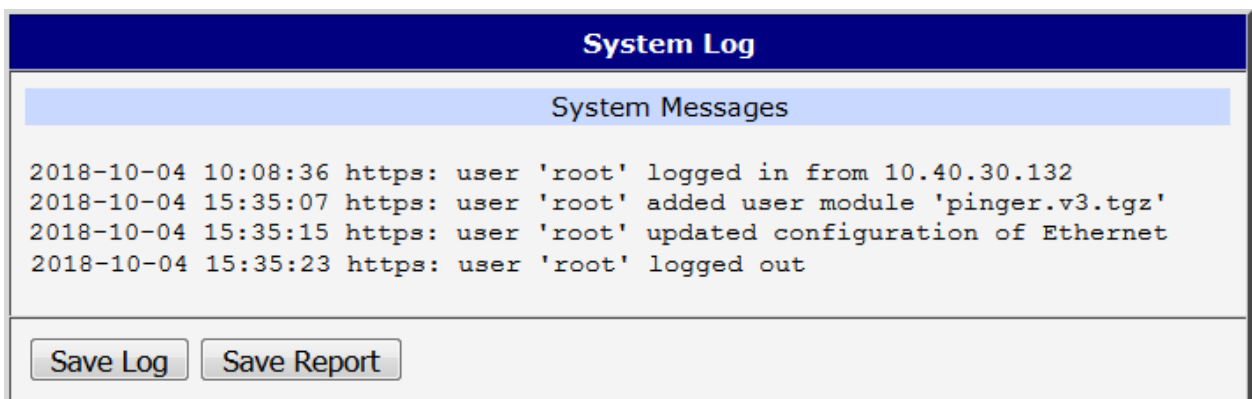
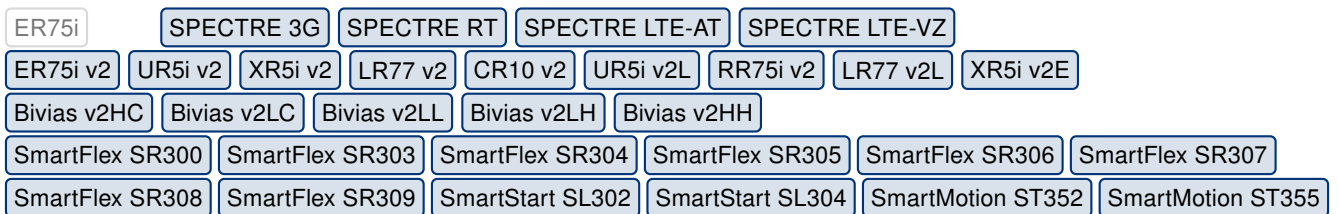


Figure 1: Example of logged actions

Added possibility to use custom HTTPS certificate



It is now possible to upload custom PEM certificate for HTTPS service including corresponding private key. The regeneration of a self-signed certificate is supported as well. Please note that the certificate validity should cover extensive time period so that you not lock yourself out of access to the Web UI in case of e.g. clock reset to 1980.

Support for network traffic mirroring

ER75i	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	SmartStart SL302	SmartStart SL304	SmartMotion ST352	SmartMotion ST355			

Support for network mirroring was added to the kernel. It can be enabled in new user module called *Ethernet Mirroring*. It allows to set network traffic mirroring from an Ethernet interface to another one. Please note that for actual mirroring to take place you need to install and enable *Ethernet Mirroring* user module.

Added *Product Type* into *status* program

ER75i	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	SmartStart SL302	SmartStart SL304	SmartMotion ST352	SmartMotion ST355			

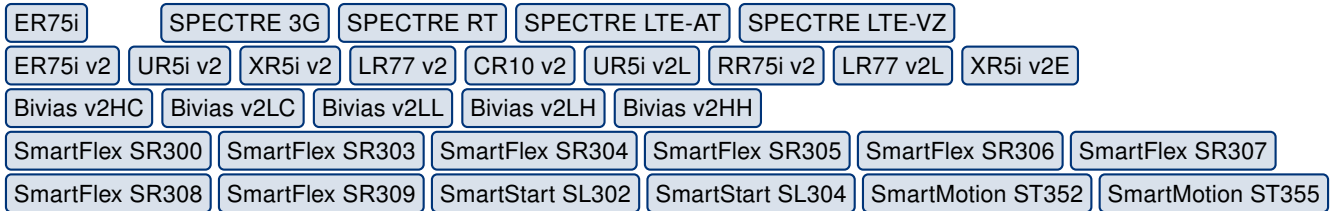
System output of the *status* program was enhanced with the information about router’s product type. Product type is represented by a code which corresponds with model of the router and its hardware configuration.

Syntax of the *status* program to list the system information including the product type entry is `status -v sys`. For more information see *Commands and Scripts* application note.

Note 1: Information about the product type is also available in report of the router, which can be generated from the GUI.

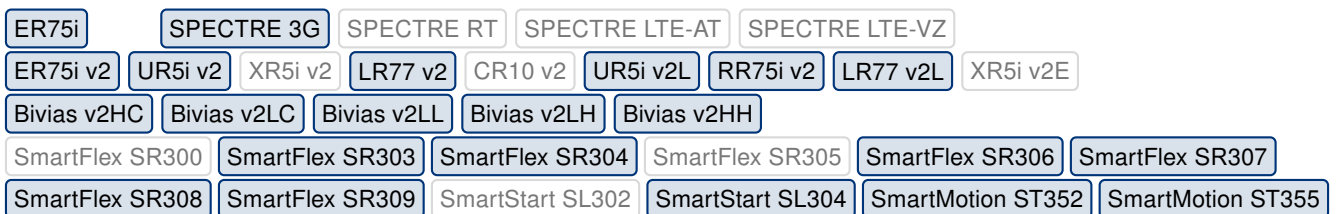
Note 2: Product type record is only available for routers produced since November 2018.

Improvements in Web GUI fields validation



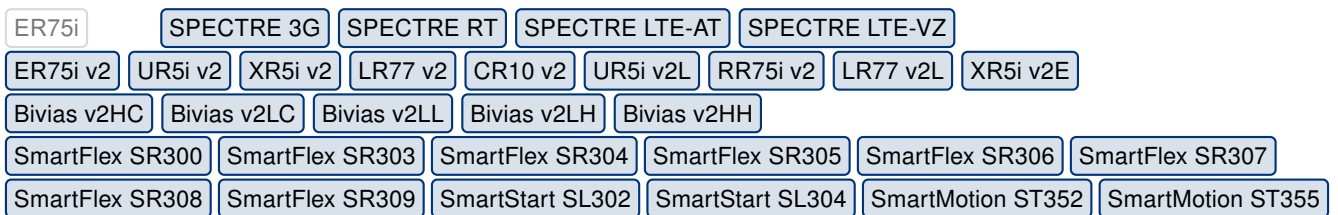
Validation function for all fields in the web GUI was improved. If a value range for the field exists, a message with expected range will be displayed in case that wrong value was entered into this field.

Changed APN entry



Default APN entry for *Telia* cellular network (PLMN 24202) was changed from *tsn* to *internet.telia.no* string.

Fixed selection of PSK for IKEv1



Fixed issue with selecting of PSK for IPsec IKEv1 Main Mode. This issue was observed in case the local or remote IP address was specified in the GUI.

Fixed update of DynDNS record

ER75i	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	SmartStart SL302	SmartStart SL304	SmartMotion ST352	SmartMotion ST355			

Fixed issue with updating of DynDNS record. If an IP address was assigned to the SIM card dynamically and the cellular connection was re-established, the DynDNS record was not updated correctly.

Fixed crashing of DHCP client

ER75i	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	SmartStart SL302	SmartStart SL304	SmartMotion ST352	SmartMotion ST355			

Fixed an issue with moving a lease from one interface to another, which was causing a crash of the DHCP client.

Fixed reading A/D converter values

ER75i	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	SmartStart SL302	SmartStart SL304	SmartMotion ST352	SmartMotion ST355			

Under heavy router load, the reading of values from A/D converter could fail. This caused the *Temperature* and *Supply Voltage* values missing in the system information section of the GUI or when getting these values by SNMP protocol.

Fixed SIM LED indication

ER75i	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	SmartStart SL302	SmartStart SL304	SmartMotion ST352	SmartMotion ST355			

Fixed state indication of SIM1 LED. This LED did not shine after the router’s reboot was performed. It was working correctly only in case the mobile WAN connection was re-established.

Fixed vulnerability in *wpa_supplicant* program

ER75i	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	SmartStart SL302	SmartStart SL304	SmartMotion ST352	SmartMotion ST355			

A security issue was discovered in *wpa_supplicant* program of version 2.0 through 2.6. Under certain conditions, the integrity of EAPOL-Key messages was not checked, leading to a decryption oracle. An attacker within range of the Access Point and client can abuse the vulnerability to recover sensitive information. For more details see [CVE-2018-14526](#).

Fixed vulnerability in Linux kernel

ER75i	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	SmartStart SL302	SmartStart SL304	SmartMotion ST352	SmartMotion ST355			

Linux kernel of version 3.9+ is vulnerable to a denial of service attack with low rates of specially modified packets targeting IP fragment re-assembly. An attacker may cause a denial of service condition by sending specially crafted IP fragments. This vulnerability became exploitable in the Linux kernel with the increase of the IP fragment reassembly queue size. For more details see [CVE-2018-5391](#) or [Vulnerability Note VU#641765](#).

Upgraded *OpenSSL* library

ER75i	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	SmartStart SL302	SmartStart SL304	SmartMotion ST352	SmartMotion ST355			

OpenSSL library was upgraded to version 1.0.2p. This update has fixed [CVE-2018-0732](#) and [CVE-2018-0737](#).

Upgraded *BusyBox* program

ER75i	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	SmartStart SL302	SmartStart SL304	SmartMotion ST352	SmartMotion ST355			

BusyBox program was upgraded to version 1.29.3. This update has fixed [CVE-2018-1000517](#).

Upgraded *Net-SNMP* program

ER75i	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	SmartStart SL302	SmartStart SL304	SmartMotion ST352	SmartMotion ST355			

Net-SNMP program was upgraded to version 5.8. This update has fixed [CVE-2018-18066](#).

Upgraded *OpenSSH* program

ER75i	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	SmartStart SL302	SmartStart SL304	SmartMotion ST352	SmartMotion ST355			

OpenSSH program was upgraded to version 7.9p1. This update has fixed [CVE-2018-15473](#) and [CVE-2018-15919](#).

Upgraded *curl* program

ER75i	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	SmartStart SL302	SmartStart SL304	SmartMotion ST352	SmartMotion ST355			

Curl program was upgraded to version 7.62.0. This update has fixed [CVE-2018-16839](#), [CVE-2018-16840](#) and [CVE-2018-16842](#).

Part III
Known Issues

5 GHz band for WiFi

The first one hundred v3 routers produced (with serial number from 6200000 to 6200099) contain a WiFi chip which does not support the 5 GHz band. There is no way of detecting this, the 5 GHz ranges on these devices will simply not work and the router will not be able to detect this.

Warning during WiFi configuration update

During a WiFi configuration update a warning may appear in syslog. This has no other known effects other than the appearance of the warning message.

Firmware Update – unexpected filename

If the filename of a firmware for your router was changed recently, you can have an issue during manual firmware updating or with Automatic Update feature. Following 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 Upgrade Instructions](#).

SmartStart – cellular network registration

It is necessary to use router's firmware of version 6.1.5 or higher if the *Telit* cellular module installed in your SmartStart router has following version 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 of version higher than 20.00.012 is required.