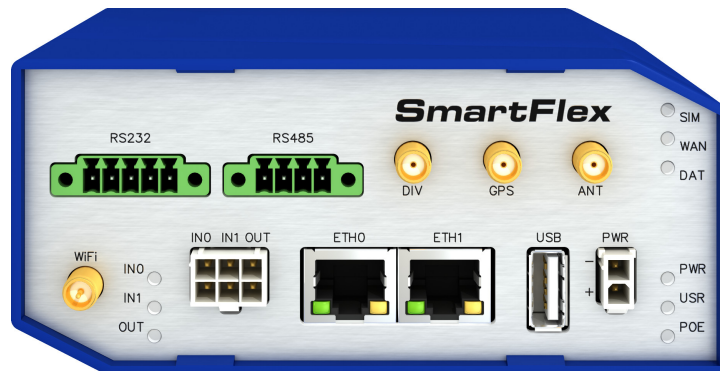# Firmware 6.1.3

RELEASE NOTES

B+B SmartWorx

Powered by ADVANTECH

Abstract

This document describes:

- Firmware upgrade instructions.

- Description of all new features, fixes and other changes implemented in firmware 6.1.3.

- Known issues.

For detailed information about firmware 6.1.3, see the Configuration Manual for your router.

Firmware Details

- **Version**: 6.1.3

- **Release date**: August 10, 2017

- **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. To get the Python user module, please contact your local Sales Representative.

> 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

4th revision of Cinterion cellular modules

ER75i | UR5 | UR5i | XR5i | SPECTRE 3G | SPECTRE RT | SPECTRE LTE-AT | SPECTRE LTE-VZ
ER75i v2 | UR5 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 SR305 | SmartFlex SR306 | SmartFlex SR307
SmartStart SL302 | SmartStart SL304 | SmartMotion ST352 | SmartMotion ST355

4th revision of *Cinterion PLS8* cellular modules made by *Gemalto* is supported from this release of the Firmware.

Clickjacking and XSS defense

ER75i | UR5 | UR5i | XR5i | SPECTRE 3G | SPECTRE RT | SPECTRE LTE-AT | SPECTRE LTE-VZ
ER75i v2 | UR5 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 SR305 | SmartFlex SR306 | SmartFlex SR307
SmartStart SL302 | SmartStart SL304 | SmartMotion ST352 | SmartMotion ST355

Defense against *Clickjacking* and *XSS* attacks was implemented. *Clickjacking* is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages. It is a browser security issue that is a vulnerability across a variety of browsers and platforms.

Important note: From now, it is not possible to use router's web interface inside another frame on a user's web page.

Delay reboot until firmware update finishes

ER75i	UR5	UR5i	XR5i		SPECTRE 3G	SPECTRE RT	SPECTRE LTE-AT	SPECTRE LTE-VZ
ER75i v2	UR5 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 SR305	SmartFlex SR306	SmartFlex SR307
SmartStart SL302	SmartStart SL304	SmartMotion ST352	SmartMotion ST355

Replaced the reboot applet in *BusyBox* with our implementation in *cbox*. It will delay the reboot while the firmware update process is in progress.

Statistic match extension for iptables

ER75i	UR5	UR5i	XR5i		SPECTRE 3G	SPECTRE RT	SPECTRE LTE-AT	SPECTRE LTE-VZ
ER75i v2	UR5 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 SR305	SmartFlex SR306	SmartFlex SR307
SmartStart SL302	SmartStart SL304	SmartMotion ST352	SmartMotion ST355

Added support for *statistic* match extension to *iptables*. This extension matches packets based on some statistic condition and is often used for data load balancing. It supports two distinct modes settable with the *–mode* option, *random* and *nth*. Visit Linux manual pages for detailed description of this extension.

Thumb instruction set

ER75i	UR5	UR5i	XR5i		SPECTRE 3G	SPECTRE RT	SPECTRE LTE-AT	SPECTRE LTE-VZ
ER75i v2	UR5 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 SR305	SmartFlex SR306	SmartFlex SR307
SmartStart SL302	SmartStart SL304	SmartMotion ST352	SmartMotion ST355

Added support for *Thumb* instruction set. *Thumb* instructions are either 16 or 32 bits long. Instructions are stored half-word aligned. Some instructions use the least significant bit of the address to determine whether the code being branched to is *Thumb* code or *ARM* code.

Disabled renegotiation of SSL connection

ER75i	UR5	UR5i	XR5i		SPECTRE 3G	SPECTRE RT	SPECTRE LTE-AT	SPECTRE LTE-VZ
ER75i v2	UR5 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 SR305	SmartFlex SR306	SmartFlex SR307
SmartStart SL302	SmartStart SL304	SmartMotion ST352	SmartMotion ST355

Disabled client-initiated renegotiation of *SSL* connection to *HTTPS* server. The reason for this change is the defense against the Denial of service (DoS) attacks.

Cellular network registration issue

ER75i	UR5	UR5i	XR5i		SPECTRE 3G	SPECTRE RT	SPECTRE LTE-AT	SPECTRE LTE-VZ
ER75i v2	UR5 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 SR305	SmartFlex SR306	SmartFlex SR307
SmartStart SL302	SmartStart SL304	SmartMotion ST352	SmartMotion ST355

Fixed an issue when, under certain conditions, the cellular connection was established even if the operator's name was not configured.

Registration to unavailable cellular network

ER75i	UR5	UR5i	XR5i		SPECTRE 3G	SPECTRE RT	SPECTRE LTE-AT	SPECTRE LTE-VZ
ER75i v2	UR5 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 SR305	SmartFlex SR306	SmartFlex SR307
SmartStart SL302	SmartStart SL304	SmartMotion ST352	SmartMotion ST355

Fixed an issue when, under certain conditions, the *MS class* on the *Telit LE910* cellular module was switched to *CC* (GSM only). This issue caused that the router was switched to the *GSM mode* only and has persisted in this mode even if the restart was performed.

8

Fixed statistic for daylight saving time adjustment

ER75i	UR5	UR5i	XR5i		SPECTRE 3G	SPECTRE RT	SPECTRE LTE-AT	SPECTRE LTE-VZ
ER75i v2	UR5 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 SR305	SmartFlex SR306	SmartFlex SR307
SmartStart SL302	SmartStart SL304	SmartMotion ST352	SmartMotion ST355

Fixed incorrect *Mobile WAN* statistic processing. Statistic from previous day was deleted after the daylight time adjustment (if the *DST* feature was enabled in *NTP* service configuration).

Configuration issue on cellular module

ER75i	UR5	UR5i	XR5i		SPECTRE 3G	SPECTRE RT	SPECTRE LTE-AT	SPECTRE LTE-VZ
ER75i v2	UR5 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 SR305	SmartFlex SR306	SmartFlex SR307
SmartStart SL302	SmartStart SL304	SmartMotion ST352	SmartMotion ST355

Made a workaround to fix bug in *Telit LE910-NA1* cellular module. This bug caused that the router was not able to connect to the *Mobile WAN* once the non-US firmware was uploaded to the router.

Communication issues on cellular modules

ER75i	UR5	UR5i	XR5i		SPECTRE 3G	SPECTRE RT	SPECTRE LTE-AT	SPECTRE LTE-VZ
ER75i v2	UR5 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 SR305	SmartFlex SR306	SmartFlex SR307
SmartStart SL302	SmartStart SL304	SmartMotion ST352	SmartMotion ST355

Fixed frozen communication on *MC7710* and *MC8705 Sierra wireless* cellular modules.

Frozen Backup Routes daemon

ER75i	UR5	UR5i	XR5i		SPECTRE 3G	SPECTRE RT	SPECTRE LTE-AT	SPECTRE LTE-VZ

ER75i v2 | UR5 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 SR305 | SmartFlex SR306 | SmartFlex SR307

SmartStart SL302 | SmartStart SL304 | SmartMotion ST352 | SmartMotion ST355

Fixed occasional freezing of the *Backup Routes* daemon. This state caused that the router was restarted within two minutes automatically.

WiFi driver fixes

ER75i | UR5 | UR5i | XR5i | SPECTRE 3G | SPECTRE RT | SPECTRE LTE-AT | SPECTRE LTE-VZ

ER75i v2 | UR5 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 SR305 | SmartFlex SR306 | SmartFlex SR307

SmartStart SL302 | SmartStart SL304 | SmartMotion ST352 | SmartMotion ST355

Fixed a few different error messages from WiFi driver in Kernel log. Besides, a few Kernel patches for WiFi driver was applied. These patches should improve the WiFi data processing.

WiFi transmit power

ER75i | UR5 | UR5i | XR5i | SPECTRE 3G | SPECTRE RT | SPECTRE LTE-AT | SPECTRE LTE-VZ

ER75i v2 | UR5 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 SR305 | SmartFlex SR306 | SmartFlex SR307

SmartStart SL302 | SmartStart SL304 | SmartMotion ST352 | SmartMotion ST355

Fixed setting of WiFi transmit power for *Sagrad* WiFi module. Transmit power is adjusted based on the *Country Code* set in router's configuration.

GRE tunnel initialization

| ER75i | UR5 | UR5i | XR5i | | SPECTRE 3G | SPECTRE RT | SPECTRE LTE-AT | SPECTRE LTE-VZ |

| ER75i v2 | UR5 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 SR305 | SmartFlex SR306 | SmartFlex SR307 |

| SmartStart SL302 | SmartStart SL304 | SmartMotion ST352 | SmartMotion ST355 |

This issue caused that the *GRE* tunnel initialization has failed on ER75i and UR5 routers. For all other routers the initialization was working, but the IP address of the interface was not set up.

IPsec tunnel termination

| ER75i | UR5 | UR5i | XR5i | | SPECTRE 3G | SPECTRE RT | SPECTRE LTE-AT | SPECTRE LTE-VZ |

| ER75i v2 | UR5 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 SR305 | SmartFlex SR306 | SmartFlex SR307 |

| SmartStart SL302 | SmartStart SL304 | SmartMotion ST352 | SmartMotion ST355 |

Fixed *IPsec* tunnel termination. This issue could cause an interruption of communication through the *IPsec* tunnel.

OpenVPN issue

| ER75i | UR5 | UR5i | XR5i | | SPECTRE 3G | SPECTRE RT | SPECTRE LTE-AT | SPECTRE LTE-VZ |

| ER75i v2 | UR5 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 SR305 | SmartFlex SR306 | SmartFlex SR307 |

| SmartStart SL302 | SmartStart SL304 | SmartMotion ST352 | SmartMotion ST355 |

Fixed crashes of *OpenVPN* daemon.

DNS translation issue

ER75i	UR5	UR5i	XR5i		SPECTRE 3G	SPECTRE RT	SPECTRE LTE-AT	SPECTRE LTE-VZ
ER75i v2	UR5 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 SR305	SmartFlex SR306	SmartFlex SR307
SmartStart SL302	SmartStart SL304	SmartMotion ST352	SmartMotion ST355

Fixed *DNS64* translation issue on interfaces without *IPv6* address configured.

OpenVPN program upgrade

ER75i	UR5	UR5i	XR5i		SPECTRE 3G	SPECTRE RT	SPECTRE LTE-AT	SPECTRE LTE-VZ
ER75i v2	UR5 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 SR305	SmartFlex SR306	SmartFlex SR307
SmartStart SL302	SmartStart SL304	SmartMotion ST352	SmartMotion ST355

Upgraded *OpenVPN* program to version 2.3.17. This update has fixed CVE-2017-7508, CVE-2017-7520 and CVE-2017-7521.

tcpdump program upgrade

ER75i	UR5	UR5i	XR5i		SPECTRE 3G	SPECTRE RT	SPECTRE LTE-AT	SPECTRE LTE-VZ
ER75i v2	UR5 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 SR305	SmartFlex SR306	SmartFlex SR307
SmartStart SL302	SmartStart SL304	SmartMotion ST352	SmartMotion ST355

Upgraded *tcpdump* program to version 4.9.1. This update has fixed CVE-2017-11108.

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.

Python user module

Python user module versions earlier than 2014-11-25 have lacked SSL functionality since firmware version 5.3.4. **The Python user module needs to be upgraded** to version from 2016-05-03 or later. This user module upgrade can be done safely either before or after upgrading the firmware. The Python interpreter version 2.7.12 is included in the latest version of the user module (2016-09-30).

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) in this document.

SmartStart SL302 cellular network authentication with username and password

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) does not support sending or receiving of SMS in Verizon cellular network.