Sierra Wireless WP77xx R15.1

Customer Release Notes

SIERRA WIRELESS®

41114680
Rev. 1.0

Important Notice

Due to the nature of wireless communications, transmission and reception of data can never be guaranteed. Data may be delayed, corrupted (i.e., have errors) or be totally lost. Although significant delays or losses of data are rare when wireless devices such as the Sierra Wireless product are used in a normal manner with a well-constructed network, the Sierra Wireless product should not be used in situations where failure to transmit or receive data could result in damage of any kind to the user or any other party, including but not limited to personal injury, death, or loss of property. Sierra Wireless accepts no responsibility for damages of any kind resulting from delays or errors in data transmitted or received using the Sierra Wireless product, or for failure of the Sierra Wireless product to transmit or receive such data.

Safety and Hazards

Do not operate the Sierra Wireless product in areas where blasting is in progress, where explosive atmospheres may be present, near medical equipment, near life support equipment, or any equipment which may be susceptible to any form of radio interference. In such areas, the Sierra Wireless product **MUST BE POWERED OFF**. The Sierra Wireless product can transmit signals that could interfere with this equipment.

Do not operate the Sierra Wireless product in any aircraft, whether the aircraft is on the ground or in flight. In aircraft, the Sierra Wireless product **MUST BE POWERED OFF**. When operating, the Sierra Wireless product can transmit signals that could interfere with various onboard systems.

Note: Some airlines may permit the use of cellular phones while the aircraft is on the ground and the door is open. Sierra Wireless products may be used at this time.

The driver or operator of any vehicle should not operate the Sierra Wireless product while in control of a vehicle. Doing so will detract from the driver or operator's control and operation of that vehicle. In some states and provinces, operating such communications devices while in control of a vehicle is an offence.

Limitation of Liability

The information in this manual is subject to change without notice and does not represent a commitment on the part of Sierra Wireless. SIERRA WIRELESS AND ITS AFFILIATES SPECIFICALLY DISCLAIM LIABILITY FOR ANY AND ALL DIRECT, INDIRECT, SPECIAL, GENERAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES INCLUDING, BUT NOT LIMITED TO, LOSS OF PROFITS OR REVENUE OR ANTICIPATED PROFITS OR REVENUE ARISING OUT OF THE USE OR INABILITY TO USE ANY SIERRA WIRELESS PRODUCT, EVEN IF SIERRA WIRELESS AND/OR ITS AFFILIATES HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR THEY ARE FORESEEABLE OR FOR CLAIMS BY ANY THIRD PARTY.

Notwithstanding the foregoing, in no event shall Sierra Wireless and/or its affiliates aggregate liability arising under or in connection with the Sierra Wireless product, regardless of the number of events, occurrences, or claims giving rise to liability, be in excess of the price paid by the purchaser for the Sierra Wireless product.

Patents

This product may contain technology developed by or for Sierra Wireless Inc. This product includes technology licensed from QUALCOMM®. This product is manufactured or sold by Sierra Wireless Inc. or its affiliates under one or more patents licensed from MMP Portfolio Licensing.

Copyright

Trademarks

Sierra Wireless®, AirLink®, AirVantage® and the Sierra Wireless logo are registered trademarks of Sierra Wireless.

Windows® and Windows Vista® are registered trademarks of Microsoft Corporation.

Macintosh® and Mac OS X® are registered trademarks of Apple Inc., registered in the U.S. and other countries.

QUALCOMM® is a registered trademark of QUALCOMM Incorporated. Used under license.

Other trademarks are the property of their respective owners.

Contact Information

Sales information and technical support, including warranty and returns	Web: sierrawireless.com/company/contact-us/ Global toll-free number: 1-877-687-7795 6:00 am to 5:00 pm PST
Corporate and product information	Web: sierrawireless.com

Revision History

Revision number	Release date	Changes
1.0	April 2023	Creation

Contents

1: About this Document

This document describes WP77xx firmware releases.These release notes may be distributed to all direct and indirect customers.

1.1 Compatibility

1.1.1 Hardware Compatibility

Product Compatibility List
WP7702 • LTE Cat-M1; Bands 1, 2, 3, 4, 5, 8, 12, 13, 18, 19, 20, 26, 28 • LTE CAT-NB1; Bands 1, 2, 3, 4, 5, 8, 12, 13, 17, 18, 19, 20, 26, 28 • GSM; Bands GSM 850, E-GSM 900, DCS 1800, PCS 1900

2: SWI9X06Y Release 15.1

Release 15.1 is a major release for WP7702.

This release brings in incremental security and Legato application framework updates.

2.1 Software Release Description

2.1.1 Release Identification

Component	Revision
Modem Firmware	SWI9X06Y_02.36.08.09 c094f4 jenkins 2022/06/24 03:14:28
Linux Firmware	SWI9X06Y_03.00.13.00 2022-12-27_09:10:00
MCU Firmware	002.015 (embedded as a binary in the Linux image)
Legato Application Framework	21.05.0
Binary Size	57.9 MB (compressed binaries)
IMEI SV	6
Qualcomm Stack Version	MDM9206.LE.2.0-00202-STD.PROD-1.372800.1.501398.1
Linux Kernel Version	Linux version 4.14.253 (oe-user@oe-host) (gcc version 9.3.0 (GCC), GNU ld (GNU Binutils) 2.34.0.20200220) #1 PREEMPT Wed Feb 16 10:15:15 UTC 2022
Supported H/W	WP7702

2.1.2 Software Tools Version

S/W Tools Name	Version
Windows Driver Package	B5087
Windows SDK	None
Skylight	None

Available in https://source.sierrawireless.com

2.1.3 Released Files

File	Carrier	Modem Firmware	Config	Linux Distribution	Base Legato System	Comment
WP7702 Approved Packages						
WP77xx_Release15.1_GENERIC.exe	GENERIC	SWI9X06Y_02.36.08.09	001.079_000	SWI9X06Y_03.00.13.00	21.05.0	GCF and PTCRB Approved
WP77xx_Release15.1_ATT.exe	ATT	SWI9X06Y_02.36.06.00	001.067_005	SWI9X06Y_03.00.13.00	21.05.0	AT&T Approved
WP77xx_Release15.1_VERIZON.exe	VERIZON	SWI9X06Y_02.22.12.00	001.042_004	SWI9X06Y_03.00.13.00	21.05.0	Verizon Approved
WP77xx_Release15.1_TELSTRA.exe	TELSTRA	SWI9X06Y_02.36.08.02	001.061_001	SWI9X06Y_03.00.13.00	21.05.0	Telstra Approved
WP77xx_Release15.1_SIERRA.exe	SIERRA	SWI9X06Y_02.36.08.09	001.049_000	SWI9X06Y_03.00.13.00	21.05.0	GCF and PTCRB Approved

Function	Files
Firmware components	9999999_9907618_SWI9X06Y_02.36.08.09_00_GENERIC_001.079_000.spk (GCF/PTCRB) 9999999_9907787_SWI9X06Y_02.36.06.00_00_ATT_001.067_005.spk 9999999_9908088_SWI9X06Y_02.22.12.00_00_VERIZON_001.042_004.spk 9999999_9907618_SWI9X06Y_02.36.08.02_00_TELSTRA_001.061_001.spk 9999999_9908788_SWI9X06Y_02.36.08.09_00_SIERRA_001.049_000.spk linux-SWI9X06Y_03.00.13.00.cwe legato-21.05.0.cwe
Available in https://source.sierrawireless.com	

2.1.4 Available Memory Flash

Name	Partition	Allocation (kb)	Image Size (kb)	Usage
Linux Kernel	mtd12 (boot)	14336	9509	66%
Linux Rootfs	mtd13 (system)	60416	23552	38%
Legato Framework	mtd14 (lefwkro)	17664	6554	37%
SWIRW	mtd15 (swirw)	15872		
USERAPP	mtd16 (userapp)	133120		

2.1.4.1 RAM

104688 kB

Note:

- *Value is read from the MemAvailable parameter in /proc/meminfo*
- *Values are for reference only and will vary depending on what services or processes are running at the time of measurement.*
- *Available memory in Flash and RAM are for reference only and may vary depending on the time of measurement and configuration changes made by customers.*

2.2 Software Changes Description

The WP7702 Release 15.1 is based on modem version SWI9X06Y_02.36.08.09 and Linux version SWI9X06Y_03.00.13.00.

This release includes the following changes and features.

Table 2-1: Major Bug Fixes

ID	Description	Impacted Domain
Various	legato-21.05.0: https://docs.legato.io/21_05/aboutReleaseNotes.html Includes: • Improves AirVantage connection reliability • Fixes various memory leaks	Legato AF
LXSWIREF-1964	[Yocto-3.1] Align meta-swi* layers to the latest in master	Linux
ECHO-1190	Add new Linux features, compatibility with latest drivers, and security patches via Linux version 4.14.	Linux
LXSWIREF-2069	Due to concerns about backwards compatibility, default firewall input policy was set to ACCEPT. While individual firewall rules protect static interfaces such as eth0 and rmnet_data0, any interface created at run time would have all ports open and hence prone to attacks.	Linux
QTI9X06-556	The ADC0 and ADC1 values read by AT!madc? are incorrect	Linux
QTI9X06-639	TAU may be rejected by the network if the PSM T3412 timer is set to 80 minutes	PSM
QTI9X06-684	at!dmcredwrite=3,"beefbeefbeefbeefbeefbeefbeefcafe",101 no response	Linux

2.3 Security Corrections / Improvements

CVE	Description
CVE-2020-25687	Heap-based buffer overflow with large memcpy when DNSSEC is enabled.
CVE-2020-25686	Remote attackers can spoof DNS traffic that can lead to DNS cache poisoning.
CVE-2020-25685	
CVE-2020-25684	Lack of proper address / port check makes forging replies easier for an off-path attacker.
CVE-2020-25683	Heap-based buffer overflow when DNSSEC is enabled can result in denial of service.
CVE-2020-25682	Remote attacker can cause memory corruption on the target device.
CVE-2020-25681	Remote attacker can write arbitrary data into target device's memory that can lead to memory corruption and other unexpected behaviors on the target device.
CVE-2019-14834	Memory leak allows remote attackers to cause a denial of service via vectors involving DHCP response creation.

2.4 Known Issues

The following table presents the known issues in this release.

ID	Title	Description	Impacted Domain
ECHO-1068	Secure store data inaccessible after downgrade	Starting from Release 11 (Legato 19.07), downgrading to an older Legato release is not supported and may cause data saved in secure store to become permanently inaccessible, even after subsequent upgrade.	Secure Storage
ECHO-847	Stopping spiService does not remove spidev and spisvc kernel module	In this release, spiService can now be started, but the spidev and spisvc kernel modules were not removed even after the service was stopped.	Driver
LE-13441	Unable to connect to AirVantage server on ATT network when profile APN is NULL	If the APN in the data profile is blank, Legato will attempt to write a carrier-specific APN into the device before attempting to connect to AirVantage. Sometimes this APN does not work with the SIM being used and, as a result, device is unable to make a data connection. As a workaround, customers should manually set the correct APN on their device instead of leaving it NULL before attempting to connect to AirVantage.	Connectivity

ID	Title	Description	Impacted Domain
ECHO-1048	AT!POWERWAKE returns unexpected wake timer value when PSM is disabled	After disabling PSM via AT+CPSMS=0 and clearing wake timers via AT!POWERWAKE=0, AT!POWERWAKE? will still return a default PSM wake timer value. This value can be ignored and modem will not wake from PSM.	PSM
ECHO-1066	UART2 driver mapping changed	When mapping services to UART2 via AT!MAPUART=17,2, the HS1 driver is now used instead of HSL1	UART
QTI9X06-696	[AUTO-SIM] AUTO-SIM feature does not work properly at 50°C	This issue impacts all carrier-switching when AUTO SIM feature is enabled. If user wants to switch a SIM card using the auto SIM feature, do it when the module temperature (AT!PCTEMP?) is under 50°C to prevent repeating module resets. If repeated resets occur, the reset behavior will only stop, and AUTO SIM will work, when the module's internal temperature (AT!PCTEMP?) is under 50°C. For example: When AUTO SIM is enabled, the FW would not switch from SIERRA to GENERIC at 50°C after replacing a SIERRA SIM with a GENERIC SIM. The module would also keep on resetting.	Connectivity

A: Appendix

A.1 Abbreviations and Definitions

Abbreviation / Acronym	Definitions
AT	Access Terminal, Attention
CVE	Common Vulnerabilities and Exposures
LK	Little Kernel Linux bootloader
FDT	Firmware Download Tool
LPWA	Low-Power Wide-Area Wireless Technology
MCU	Microcontroller Unit - An onboard MCU enables Ultra Low Power modes of operation
PSM	Power Save Mode
QMI	Qualcomm MSM Interface, Qualcomm Modem Interface
ULPS	Ultra Low Power State

A.2 Related Documentation

- WP77xx - Product Technical Specification
  Reference number: 41111420
- WPx5xx-76xx-77xx AT Command Reference
  Reference number: 4118047
- WP Series - Preparing Your Devices for Deployment
  Reference number: 41110380
- WPX5-76-77 Scalability Guide
  Reference number: 41110866
- WP76xx Customer Release Notes
  Reference number: 41110418