



WP77xx

Customer Release Notes

Release 13

| | |
|-----------------|------------|
| Document number | 41111700 |
| Rev | R01.09 |
| Date | 2020/07/30 |

Document History

| Rev XX.YY | Date YYYY/MM/DD | Updates | Author |
|--------------|--------------------|--|-----------------|
| 01.09 | 2020/07/30 | Updated Legato Version for Release 13 | BN |
| 01.08 | 2020/07/16 | Release 13 | AV / SV / KW |
| 01.07 | 2019/09/06 | Release 12 | SL |
| 01.06 | 2019/05/31 | Added WP7702 Verizon Package to Release 11 | SL |
| 01.05 | 2019/05/07 | Release 11 | SL |
| 01.04 | 2018/07/27 | Release 9.1 | SL |
| 01.03 | 2018/05/25 | Release 9 | SL |
| 01.02 | 2018/02/28 | Release 8 | SL |
| 01.01 | 2017/12/29 | Release 7 | SL |
| 01.00 | 2017/10/23 | Creation - Release 6 | SL |

Table of Contents

| | | |
|------------------|---|------------------|
| <u>1</u> | <u>INTRODUCTION</u> | <u>4</u> |
| <u>2</u> | <u>ABBREVIATIONS AND DEFINITIONS</u> | <u>4</u> |
| <u>3</u> | <u>RELATED DOCUMENTATION</u> | <u>4</u> |
| <u>4</u> | <u>COMPATIBILITY</u> | <u>5</u> |
| <u>5</u> | <u>SWI9X06Y RELEASE 13</u> | <u>6</u> |
| <u>6</u> | <u>SWI9X06Y RELEASE 12</u> | <u>17</u> |
| <u>7</u> | <u>SWI9X06Y RELEASE 11</u> | <u>38</u> |
| <u>8</u> | <u>SWI9X06Y RELEASE 9.1</u> | <u>49</u> |
| <u>9</u> | <u>SWI9X06Y RELEASE 9</u> | <u>55</u> |
| <u>10</u> | <u>SWI9X06Y RELEASE 8</u> | <u>59</u> |
| <u>11</u> | <u>SWI9X06Y RELEASE 7</u> | <u>62</u> |
| <u>12</u> | <u>SWI9X06Y RELEASE 6</u> | <u>66</u> |
| <u>13</u> | <u>TROUBLESHOOTING</u> | <u>70</u> |
| <u>14</u> | <u>CERTIFICATION DESCRIPTION</u> | <u>70</u> |
| <u>15</u> | <u>RESTRICTIONS AND ADDITIONAL INFORMATION</u> | <u>70</u> |

1 Introduction

1.1 Scope of this document

This document describes WP77xx firmware releases.

1.2 Audience of this document

These release notes may be distributed to all direct and indirect customers.

2 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 |

3 Related documentation

| Ref. # | Doc. # | Document title |
|--------|----------|--|
| [1] | 41111420 | AirPrime WP77xx - Product Technical Specification |
| [2] | 4118047 | AirPrime WPx5xx/WP76xx/WP77xx - AT Command Reference |
| [3] | 41110380 | AirPrime WP Series – Preparing Your Devices For Deployment |
| [4] | 41110866 | AirPrime WPx5xx/WP76xx/WP77xx - Scalability Guide |
| [5] | 41110418 | AirPrime WP76xx Customer Release Notes |

4 Compatibility

Hardware compatibility

| Product compatibility list |
|---|
| <p>WP7702</p> <ul style="list-style-type: none"> • <i>LTE Cat-M1; Bands 1, 2, 3, 4, 5, 8, 12, 13, 18, 19, 20, 26, 28</i> • <i>LTE CAT-NB1; Bands 1, 2, 3, 4, 5, 8, 12, 13, 17, 18, 19, 20, 26, 28</i> • <i>GSM; Bands GSM 850, E-GSM 900, DCS 1800, PCS 1900</i> <p>WP7700</p> <ul style="list-style-type: none"> • <i>LTE Cat-M1; Bands 1, 2, 3, 4, 5, 8, 12, 13, 18, 19, 20, 26, 28</i> • <i>LTE CAT-NB1; Bands 1, 2, 3, 4, 5, 8, 12, 13, 17, 18, 19, 20, 26, 28</i> |



5 SWI9X06Y Release 13

Release 13 is a major release for WP77xx. This release brings in a new Qualcomm stack and incremental improvements in Yocto 2.5. Both improvements provide a significant number of security enhancements. There are also improvements to R2C and FOTA functionality. MCU FW is updated to version 002.014 to solve a stability issue during I2C stress testing.

5.1 Software Release Description

5.1.1 Release identification

| Component | Revision |
|------------------------------|--|
| Modem Firmware | SWI9X06Y_02.35.02.00 5208b3 jenkins 2020/06/10 00:30:12 |
| Linux Firmware | SWI9X06Y_02.35.02.00 2020-06-10_04:06:00 |
| MCU Firmware | 002.014 (embedded as a binary in the Linux image, not distributed as a separate component) |
| Legato Application Framework | 19.11.2_625c7d1acfd1ca45b2dbe189b4cb1ce7 |
| Binary Size | 56.4MB (compressed binaries) |
| IMEI SV | 5 |
| Qualcomm Stack Version | MDM9206.LE.2.0-00192-STD.PROD |
| Linux Kernel Version | Linux swi-mdm9x28-wp 3.18.140 #1 PREEMPT Wed Jun 10 03:41:13 UTC 2020 armv7l GNU/Linux |
| Supported H/W | WP7702, WP7700 |

5.1.2 Software Tools Versions

| S/W Tools Name | Version |
|------------------------|--------------|
| Windows Driver Package | B4956 |
| Windows SDK | None |
| Skylight | None |
| Linux Drivers | S2.40N2.61 |
| Linux SDK | SLQS04.00.24 |

5.1.3 Released Files and Download Processes

| Files | Carrier | Modem Firmware | Config | Linux Distribution | Base Legato System | Comment |
|--|--------------------|----------------------|-------------|----------------------|--------------------|-----------------------|
| WP7702 Approved | | | | | | |
| WP77xx_Release 13_GENERIC_TM OBILE.exe | GENERIC (T-Mobile) | SWI9X06Y_02.13.02.00 | 001.009_001 | SWI9X06Y_02.35.02.00 | 19.11.2 | T-Mobile USA Approved |
| WP77xx_Release 13_GENERIC_GC F.exe | GENERIC (GCF) | SWI9X06Y_02.35.02.00 | 001.064_001 | SWI9X06Y_02.35.02.00 | 19.11.2 | GCF Approved |
| WP77xx_Release 13_GENERIC_PT CRB.exe | GENERIC (PTCRB) | SWI9X06Y_02.16.06.00 | 001.028_004 | SWI9X06Y_02.35.02.00 | 19.11.2 | PTCRB Approved |

| | | | |
|-------------|---------|-----------|-------|
| Template #: | 4124005 | Revision: | 01.06 |
|-------------|---------|-----------|-------|



| Files | Carrier | Modem Firmware | Config | Linux Distribution | Base Legato System | Comment |
|---|----------------------------|----------------------|-------------|----------------------|--------------------|---------------------------|
| WP77xx_Release 13_SIERRA.exe | SIERRA | SWI9X06Y_02.35.02.00 | 001.036_001 | SWI9X06Y_02.35.02.00 | 19.11.2 | GCF Approved |
| WP77xx_Release 13_ATT.exe | ATT | SWI9X06Y_02.16.06.00 | 001.026_001 | SWI9X06Y_02.35.02.00 | 19.11.2 | AT&T Approved |
| WP77xx_Release 13_GENERIC_DT.exe | GENERIC (Deutsche Telekom) | SWI9X06Y_02.22.02.00 | 001.041_001 | SWI9X06Y_02.35.02.00 | 19.11.2 | Deutsche Telekom Approved |
| WP77xx_Release 13_VERIZON.exe | VERIZON | SWI9X06Y_02.22.12.00 | 001.042_001 | SWI9X06Y_02.35.02.00 | 19.11.2 | Verizon Approved |
| WP7700 Approved | | | | | | |
| WP77xx_Release 13_GENERIC_GC F.exe | GENERIC (GCF) | SWI9X06Y_02.35.02.00 | 001.064_001 | SWI9X06Y_02.35.02.00 | 19.11.2 | GCF Approved |
| WP77xx_Release 13_GENERIC_PT CRB.exe | GENERIC (PTCRB) | SWI9X06Y_02.16.06.00 | 001.028_004 | SWI9X06Y_02.35.02.00 | 19.11.2 | PTCRB Approved |
| WP77xx_Release 13_SIERRA.exe | SIERRA | SWI9X06Y_02.35.02.00 | 001.036_001 | SWI9X06Y_02.35.02.00 | 19.11.2 | GCF Approved |
| WP77xx_Release 13_ATT.exe | ATT | SWI9X06Y_02.16.06.00 | 001.026_001 | SWI9X06Y_02.35.02.00 | 19.11.2 | AT&T Approved |
| WP77xx_Release 13_VERIZON.exe | VERIZON | SWI9X06Y_02.22.12.00 | 001.042_001 | SWI9X06Y_02.35.02.00 | 19.11.2 | Verizon Approved |
| From: https://source.sierrawireless.com/resources/airprime/software/wp77xx/wp77xx-firmware-release-13 | | | | | | |

| Function | Files |
|---|--|
| Firmware Components | 9999999_9907618_SWI9X06Y_02.13.02.00_00_GENERIC_001.009_001.spk (T-Mobile USA) 9999999_9907618_SWI9X06Y_02.16.06.00_00_GENERIC_001.028_004.spk (PTCRB) 9999999_9907618_SWI9X06Y_02.22.02.00_00_GENERIC_001.041_001.spk (Deutsche Telekom) 9999999_9907618_SWI9X06Y_02.35.02.00_00_GENERIC_001.064_001.spk (GCF) 9999999_9908788_SWI9X06Y_02.35.02.00_00_SIERRA_001.036_001.spk 9999999_9907787_SWI9X06Y_02.16.06.00_00_ATT_001.026_001.spk 9999999_9908088_SWI9X06Y_02.22.12.00_00_VERIZON_001.042_001.spk linux-SWI9X06Y_02.35.02.00.cwe legato-19.11.2.cwe |
| From: https://source.sierrawireless.com/resources/airprime/software/wp77xx/wp77xx-firmware-release-13 | |

5.1.4 Available Memory

Flash:

| NAME | PARTITION | ALLOCATION (KB) | IMG SIZE (KB) | USAGE |
|------------------|-----------------|-----------------|---------------|-------|
| Linux Kernel | mtd12 (boot) | 14336 | 9517 | 66% |
| Linux Rootfs | mtd13 (system) | 60416 | 23552 | 38% |
| Legato Framework | mtd14 (lefwkro) | 17664 | 6401 | 36% |
| SWIRW | mtd15 (swirw) | 15872 | | |
| USERAPP | mtd16 (userapp) | 133120 | | |

RAM:

104772 kB^{[1][2]}

[1] Value is read from the MemAvailable parameter in /proc/meminfo

[2] Values are for reference only and will vary depending on what services/processes are running at the time of measurement

Available of memory in Flash & RAM are for reference only and may vary depending at time of measuring and configuration changes made by customers.

| | | | |
|-------------|---------|-----------|-------|
| Template #: | 4124005 | Revision: | 01.06 |
|-------------|---------|-----------|-------|

5.2 Software Changes Description

The WP77xx Release 13 is based on modem and Linux versions SWI9X06Y_02.35.02.00.

| ID | Title | Description | Impacted Domain |
|---------------------------|---|---|-------------------|
| Legato | | | |
| Various | Legato 19.11.2 | Legato 19.11.2: https://legato.io/releases Upgrade from 19.07.0 in Release 12. | Legato AF |
| QT19X06-225 ECHO-864 | Enlarge RootFS and Legato partition for larger customer application | Modules on newer SKUs will have a larger RootFS and Legato partition, providing increased flexibility for larger custom Linux/Legato builds. Field upgrade will not modify partitions. | FOTA |
| SWIMDM-233 ECHO-833 | Dynamic configuration of customer partitions | Added support for AT!PARTITION to allow customers to resize Linux and Legato partitions in the customer factory | Legato / Linux |
| Linux Distribution | | | |
| Various | Upgrade Linux Distro to LXSWI2.5-13.1, based on Yocto 2.5 | Upgrade from LXSWI2.5-9.0 (Release 12). | Yocto baseline |
| QT19X06-349 ECHO-931 | CPU Frequency Scaling governor does not work as expected | power_config file did not include the chip ID used on WP77xx modules, preventing the Linux CPU from dynamically scaling the frequency. This resulted in higher power consumption than necessary when idle. | Power Consumption |
| QT19X06-319 ECHO-873 | Occasionally unable to wake from ULPM | Fixed a race condition in MCU driver where the system may fail to wake from ULPM. | MCU ULPM |
| QT19X06-294 | Kernel panic on bootup | Implement Workaround for Kernel Panic on Bootup Caused by BAM DMux Disconnect Timeout. Observed with custom Legato applications that take slightly longer to start up. | Linux Stability |
| ECHO-968 | I2C NACK | When writing to some GPIOs, the Linux serial console and dmesg output was flooded with I2C NACK messages. This message was innocuous but cluttered the log file making it difficult to read. | Linux debugging |
| ECHO-841 | Linux source on Leaf | Fixed issue with incomplete source delivery to Leaf | Linux |
| MCU FW | | | |
| ECHO-840 SWIMDM-609 | Update MCU FW to version 002.014 | MCU FW Version has been updated to 002.014 in this release. Includes bug fix: <ul style="list-style-type: none"> MCU-105 - Boot loop when reset by MCU Watchdog <p>If MCU Watchdog is enabled, the system may reboot repeatedly and enter Smart Error Detection mode.</p> | MCU FW |
| Modem | | | |
| Core | | | |

| ID | Title | Description | Impacted Domain |
|---|--|--|-------------------|
| Various | Multiple Qualcomm stack updates to: MDM9206.LE.2.0-00192-STD.PROD-1 | Add Qualcomm baseline MDM9206.LE.2.0-00192-STD.PROD-1 Includes: <ul style="list-style-type: none"> • QT19X06-276 - Data drop unexpectedly when DL data or AT command response is longer than CMUX N1 frame size • QT19X06-244 - Fix handling of CMUX MSC frames from host • QT19X07-3199 – Fix intermittent secure storage failure when item size is greater than 1024 bytes • QT19X28-6648 – Fix issue where thermal engine IRQ may occur more frequently than expected at specific temperatures • AT&T and Verizon critical CRs • Numerous security CVE fixes | Qualcomm baseline |
| Protocol/Certification | | | |
| QT19X06-353 | Increase IMEI SV to 5 | The IMEI SV has been increased to 5 in this release. | IMEI SV |
| SWIMDM-1355 | Update TS.25 list to April 13, 2020 | Default TS.25 list updated. Non-GSMA PLMNs removed except Test PLMNs. | GCF |
| QMI | | | |
| QT19X06-228 | Update QMI command to read HW revision | Fix hardware revision returned by QMI_DMS_GET_DEVICE_HARDWARE_REV | QMI |
| GNSS | | | |
| QT19X06-252 QT19X06-267 | Default NMEA settings | Update default NMEA settings to report all supported constellations rather than only GPS (AT!GPSNMEASENCE) | NMEA |
| I/O | | | |
| QT19X06-237 ECHO-871 ECHO-877 ECHO-897 ECHO-904 | Memory leak in UART | Fixed a memory leak in the UART RTS ISR | UART |
| QT19X06-297 | UART auto-sleep with CMUX | Fixed the issue where UART will still auto-sleep when AT!MUXMODE=1 even when disabled by AT+KSLEEP=2 | CMUX |
| SWIMDM-281 | Streamline ADC2/ADC3 measurements | Reduces the number of queries on the I2C bus when reading ADC2 and ADC3 | ADC |
| SWIMDM-277 | GPIO4 and UICC2 | Ignore AT+WIOCFG on GPIO4 when UICC2 is enabled | GPIO |
| AT Commands | | | |
| QT19X06-240 | AT!DA commands | Improve syntax checking on a variety of AT!DA commands | Diagnostics |
| QT19X06-241 QT19X06-242 | AT!DALSPARANGE | Improve bounds checking on AT!DALSPARANGE command | Diagnostics |
| QT19X06-270 ECHO-940 | AT+CLCK and "PN" | Fixed an issue where AT+CLCK command is unable to unlock "PN" facility | 3GPP |
| QT19X06-315 ECHO-892 | AT!DASCHAN channel response | Corrected the channel response returned by AT!DASCHAN | Diagnostics |
| ECHO-867 SWIMDM-575 | AT!FWD reliability | Fixed mutex issue causing unreliability in AT!FWD command | Linux AT |

| | | | |
|-------------|---------|-----------|-------|
| Template #: | 4124005 | Revision: | 01.06 |
|-------------|---------|-----------|-------|



| ID | Title | Description | Impacted Domain |
|--------------------------|--------------------------------|---|------------------|
| SWIMDM-477 | AT+KGSN | Add support for AT+KGSN command | Diagnostics |
| SWIMDM-589 | Improve GNSS URC reliability | Improved interactions between GNSS URC and asynchronous AT commands | GNSS |
| SWIMDM-305 | AT!GPSNMEACONFIG | Improve bounds checking on AT!GPSNMEACONFIG | GNSS |
| SWIMDM-591 | AT+VZWAPNE | Updated AT+VZWAPNE for optional arguments | Verizon |
| SWIMDM-555 | AT+CESQ | Updated AT+CESQ return value for RXLEV | Diagnostics |
| SWIMDM-548 SWIMDM-729 | AT+KCCINFO | Add support for AT+KCCINFO | Diagnostics |
| SWIMDM-487 | AT+CPWROFF | Add support for AT+CPWROFF | Power |
| SWIMDM-537 | AT!PCINFO | Update AT!PCINFO to include RF calibration check | Diagnostics |
| SWIMDM-1189 | AT!GETBAND | Update AT!GETBAND to prepend RAT (e.g. LTE) before the band number | Diagnostics |
| SWIMDM-432 | AT!GNSSCONFIG | Add QZSS support to AT!GNSSCONFIG | GNSS |
| Factory/Configuration | | | |
| QT19X06-363 ECHO-943 | Firmware download using xmodem | Fix regression in Release 12 where firmware download via xmodem (AT+WFWUPD) fails | Firmware upgrade |

5.3 Security Corrections/Improvements

| CVE | Description |
|-------------------------------|--|
| CVE-2020-3703 | Buffer Over-read Issue in Bluetooth Firmware(Sweyntooth issue 6.1,6.4) |
| CVE-2020-3699 | Buffer Copy Without Checking Size of Input in WLAN |
| CVE-2020-3698 | Improper Input Validation in WLAN Host |
| CVE-2020-3696 | Use After Free Issue in WLAN Host |
| CVE-2020-3688 | Buffer Over-read issue in Video |
| CVE-2020-3670 | Buffer Over-read Issue in Multi Mode Call Processor |
| CVE-2020-3666 | Stack-based Buffer overflow in WLAN |
| CVE-2020-3665 | Improper Validation of Array Index in WLAN HOST |
| CVE-2020-3663 | Buffer Copy Without Checking Size of Input in Video |
| CVE-2020-3661 | Buffer over-read Issue in Video |
| CVE-2020-3660 | Improper Validation of Array Index in Video |
| CVE-2020-3658 | Buffer Over Read Issue in Video |
| CVE-2020-3657 | Buffer Copy Without Checking Size of Input in HLOS Data |
| CVE-2020-3651 | Reachable Assertion in WLAN |
| CVE-2020-3644 | Information Exposure in Content Protection |
| CVE-2020-3643 | Information Exposure in Content Protection |
| CVE-2020-3641 | Buffer Copy Without Checking Size of input in Video |
| CVE-2020-3634 | Integer Underflow Issue in Multi Mode Call Processor |

| | | | |
|-------------|---------|-----------|-------|
| Template #: | 4124005 | Revision: | 01.06 |
|-------------|---------|-----------|-------|

| CVE | Description |
|--------------------------------|---|
| CVE-2020-3633 | Improper Validation of Array Index in Video |
| CVE-2020-3630 | Improper Validation of Array Index in Video |
| CVE-2020-3624 | Integer Overflow or Wraparound Issue in Storage |
| CVE-2020-3622 | Improper Input Validation issue in Qualcomm IPC |
| CVE-2020-3621 | Improper Validation of Array Index in Qualcomm IPC |
| CVE-2020-3620 | Integer Overflow or Wraparound in Qualcomm IPC |
| CVE-2020-3619 | Time-of-check Time-of-use Race Condition in Graphics |
| CVE-2020-3616 | Buffer Copy Without Checking Size of Input in Display |
| CVE-2020-3615 | Reachable Assertion in WLAN |
| CVE-2020-3614 | Integer Overflow or Wraparound issue in WLAN |
| CVE-2020-11144 | Buffer Over-read in Data Modem |
| CVE-2020-11132 | Buffer Over read Issue in Boot |
| CVE-2020-11131 | Integer Overflow to Buffer Overflow in WLAN |
| CVE-2020-11123 | Cryptographic Issue in HLOS |
| CVE-2020-11118 | Information Exposure Issues in WLAN |
| CVE-2020-11116 | Buffer Copy Without Checking Size of Input in WLAN |
| CVE-2020-11115 | Information Exposure Issue in WLAN |
| CVE-2019-9499 | The implementations of EAP-PWD in wpa_supplicant EAP Peer, when built against a crypto library missing explicit validation on imported elements, do not validate the scalar and element values in EAP-pwd-Commit. |
| CVE-2019-9498 | The implementations of EAP-PWD in hostapd EAP Server, when built against a crypto library missing explicit validation on imported elements, do not validate the scalar and element values in EAP-pwd-Commit. |
| CVE-2019-9497 | The implementations of EAP-PWD in hostapd EAP Server and wpa_supplicant EAP Peer do not validate the scalar and element values in EAP-pwd-Commit. |
| CVE-2019-9495 | Add helper functions for constant time operations |
| CVE-2019-9494 | Add helper functions for constant time operations |
| CVE-2019-9494 | SAE side-channel attacks |
| CVE-2019-5436 | A heap buffer overflow in the TFTP receiving code allows for DoS or arbitrary code execution in libcurl. |
| CVE-2019-2333 | Buffer Copy Without Checking Size of Input in IPA driver |
| CVE-2019-2307 | Buffer Over-read in WLAN |
| CVE-2019-2305 | Buffer Over-read Issue in WLAN |
| CVE-2019-2292 | Buffer Copy Without Checking Size of Input in WLAN |
| CVE-2019-2276 | Buffer Over-read Issue in WLAN |
| CVE-2019-2269 | Stack-based Buffer Overflow in WLAN |
| CVE-2019-2268 | Buffer Over-read in WLAN |
| CVE-2019-2253 | Improper Input Validation in Video |
| CVE-2019-1552 | For OpenSSL versions 1.1.0 and 1.1.1, the mingw configuration targets assume that resulting programs and libraries are installed in a Unix-like environment and the default prefix for program installation as well as for OPENSSLDIR should be '/usr/local'. |

| CVE | Description |
|--------------------------------|---|
| CVE-2019-14135 | Buffer Copy Without Checking Size of Input in WLAN |
| CVE-2019-14127 | Buffer Copy Without Checking Size of Input in Video |
| CVE-2019-14120 | Cryptographic Issue in Core |
| CVE-2019-14115 | Information Exposure in Content Protection |
| CVE-2019-14114 | Integer Overflow to Buffer Overflow Issue in WLAN |
| CVE-2019-14113 | Integer Overflow to Buffer Overflow Issue in WLAN |
| CVE-2019-14110 | Buffer Copy Without Checking Size of Input in WLAN |
| CVE-2019-14101 | Improper Input Validation in Diag Services |
| CVE-2019-14098 | Buffer Copy Without Checking Size of Input in WLAN |
| CVE-2019-14095 | Buffer Copy Without Checking Size of Input in Bluetooth SOC |
| CVE-2019-14094 | Buffer Over read Issue in Diag Services |
| CVE-2019-14093 | Improper Validation of Array Index in Display |
| CVE-2019-14076 | Buffer Copy Without Checking Size of Input in TrustZone |
| CVE-2019-14074 | Integer Overflow or Wraparound Issue in Diag Services |
| CVE-2019-14073 | Buffer Copy Without Checking Size of Input in Modem Data |
| CVE-2019-14070 | Use After Free Issue in Audio |
| CVE-2019-14067 | Information Exposure in QTEE |
| CVE-2019-14065 | Double Free Issue in TrustZone |
| CVE-2019-14062 | Buffer Copy Without Checking Size of Input in Multi Mode Call Processor |
| CVE-2019-14061 | Buffer Over-read Issue in Video |
| CVE-2019-14060 | Access of Uninitialized Pointer in Audio |
| CVE-2019-14057 | Buffer Copy Without Checking Size of Input in Video |
| CVE-2019-14055 | Use After Free Issue in Diag Services |
| CVE-2019-14053 | Buffer Over-read Issue in HLOS Data |
| CVE-2019-14041 | Buffer Copy Without Checking Size of Input in QTEE |
| CVE-2019-14040 | Use after free issue in QSEE |
| CVE-2019-14039 | Buffer Over-read Issue in Audio |
| CVE-2019-14038 | Buffer Over-read Issue in Audio |
| CVE-2019-14037 | Use After Free Issue in HLOS Data |
| CVE-2019-14033 | Buffer Over-read Issue in Multi Mode Call Processor |
| CVE-2019-14032 | Use After Free Issue in Audio |
| CVE-2019-14031 | Buffer Copy Without Checking Size of Input in WLAN |
| CVE-2019-14028 | Buffer Copy Without Checking Size of Input in WLAN |
| CVE-2019-14026 | Buffer Copy without checking size of input in WLAN |
| CVE-2019-14022 | Reachable Assertion in Modem Data |
| CVE-2019-14021 | Buffer Copy Without Checking Size of Input in GPS Subsystem |
| CVE-2019-14020 | Buffer over-read Issue in Multi Mode Call Processor |

| CVE | Description |
|--------------------------------|---|
| CVE-2019-14019 | Buffer over-read Issue in Multi Mode Call Processor |
| CVE-2019-14017 | Buffer Copy Without Checking Size of Input in Video |
| CVE-2019-14016 | Integer Overflow to Buffer Overflow in Video |
| CVE-2019-14013 | Buffer Copy Without Checking Size of Input in Video |
| CVE-2019-14011 | Buffer Over-read Issue in Multi Mode Call Processor |
| CVE-2019-14007 | Information Exposure Issue in Content Protection |
| CVE-2019-14006 | Improper Input Validation in Video |
| CVE-2019-14005 | Buffer Copy Without Checking Size of Input in Video |
| CVE-2019-14004 | Improper Input Validation in Video |
| CVE-2019-14003 | Improper Input Validation in Video |
| CVE-2019-14001 | Cryptographic Issue in HLOS |
| CVE-2019-14000 | Information Exposure Issue in Qualcomm IPC |
| CVE-2019-13999 | Integer Overflow or Wraparound in Qualcomm IPC |
| CVE-2019-13998 | Integer Overflow or Wraparound Issue in Qualcomm IPC |
| CVE-2019-13995 | Integer Overflow or Wraparound Issue in Trustzone |
| CVE-2019-13994 | Integer Overflow or Wraparound Issue in Trustzone |
| CVE-2019-13012 | The keyfile settings backend in GNOME GLib creates directories using <code>g_file_make_directory_with_parents (kfsb->dir, NULL, NULL)</code> and files using <code>g_file_replace_contents (kfsb->file, contents, length, NULL, FALSE, G_FILE_CREATE_REPLACE_DESTINATION, NULL, NULL, NULL)</code> . This is similar to CVE-2019-12450. |
| CVE-2019-12900 | BZ2_decompress in decompress.c has an out-of-bounds write when there are many selectors. |
| CVE-2019-12749 | dbus before 1.10.28, 1.12.x before 1.12.16, and 1.13.x before 1.13.12, as used in DBusServer in Canonical Upstart in Ubuntu 14.04 (and in some, less common, uses of dbus-daemon), allows cookie spoofing because of symlink mishandling in the reference implementation of DBUS_COOKIE_SHA1 in the libdbus library. (This only affects the DBUS_COOKIE_SHA1 authentication mechanism.) |
| CVE-2019-12450 | file_copy_fallback in gio/gfile.c in GNOME GLib does not properly restrict file permissions while a copy operation is in progress. |
| CVE-2019-11555 | The EAP-pwd implementation in hostapd (EAP server) before 2.8 and wpa_supplicant (EAP peer) before 2.8 does not validate fragmentation reassembly state properly for a case where an unexpected fragment could be received. |
| CVE-2019-10625 | Buffer Over-read Issue in Diag Services |
| CVE-2019-10622 | Buffer Over-read issue in Audio |
| CVE-2019-10616 | Null Pointer Dereference Issue in Trustzone |
| CVE-2019-10615 | Integer Overflow to Buffer Overflow in Trusted Application |
| CVE-2019-10614 | Use of Out-of-range Pointer Offset in Video |
| CVE-2019-10611 | Integer Overflow to Buffer Overflow Issue in Video |
| CVE-2019-10605 | Buffer Copy Without Checking Size of Input in WLAN Host |
| CVE-2019-10603 | Use After Free Issue in HLOS Data |
| CVE-2019-10602 | Use After Free Issue in Display |
| CVE-2019-10600 | Null Pointer Dereference Issue in WLAN Host |

| | | | |
|-------------|---------|-----------|-------|
| Template #: | 4124005 | Revision: | 01.06 |
|-------------|---------|-----------|-------|

| CVE | Description |
|----------------------------------|---|
| CVE-2019-10594 | Improper Validation of Array Index in Data Modem |
| CVE-2019-10592 | Integer Overflow to Buffer Overflow Issue in Display |
| CVE-2019-10591 | Improper Validation of Array Index in Video |
| CVE-2019-10590 | Improper Validation of Array Index Issue in Video |
| CVE-2019-10588 | Buffer Copy Without Checking Size of Input in Data Modem |
| CVE-2019-10587 | Buffer Copy Without Checking Size of Input in Data Modem |
| CVE-2019-10586 | Buffer Copy Without Checking Size of Input in Data Modem |
| CVE-2019-10584 | Buffer Over-read Issue in Video Driver |
| CVE-2019-10579 | Buffer Over-read in Video |
| CVE-2019-10578 | Improper Input Validation in Video |
| CVE-2019-10574 | Buffer Over-read Issue in QTEE keymaster |
| CVE-2019-10572 | Use of Out-of-range Pointer Offset in Video |
| CVE-2019-10571 | Buffer Copy Without Checking Size of Input in Graphics |
| CVE-2019-10567 | Configuration Issue in Linux Graphics |
| CVE-2019-10561 | Configuration Issue in Content Protection |
| CVE-2019-10558 | Improper Restriction of Operation Within the Bounds of a Memory Buffer in DSP Services |
| CVE-2019-10555 | Buffer Copy Without Checking Size of Input in Display |
| CVE-2019-10553 | Buffer Over-read Issue in Multi-mode Call processor |
| CVE-2019-10547 | Uncontrolled Resource Consumption in Kernel |
| CVE-2019-10544 | Possible out of bound access while processing get build mask command |
| CVE-2019-10538 | Improper Input Validation Issue in WLAN HOST |
| CVE-2019-10536 | Use After Free Issue in WLAN Host |
| CVE-2019-10527 | Improper Validation of Array Index in Qualcomm IPC |
| CVE-2019-10526 | Improper Validation of Array Index in WLAN |
| CVE-2019-10513 | Null Pointer Dereference Issue in Trustzone |
| CVE-2019-10512 | Improper Validation of Array Index in Audio |
| CVE-2019-10503 | Improper Validation of Array Index in Camera |
| CVE-2019-10494 | Time-of-Check Time-of-Use Race Condition in Camera |
| CVE-2019-10493 | Buffer Copy Without Checking Size of Input in GPS Module |
| CVE-2019-10483 | Information Exposure issue in QTEE |
| CVE-2019-1000020 | libarchive version commit 5a98dcf8a86364b3c2c469c85b93647dfb139961 onwards (version v2.8.0 onwards) contains a CWE-835: Loop with Unreachable Exit Condition ('Infinite Loop') vulnerability in ISO9660 parser, archive_read_support_format_iso9660.c, read_CE()/parse_rockridge() that can result in DoS by infinite loop. |
| CVE-2019-1000019 | libarchive version commit bf9aec176c6748f0ee7a678c5f9f9555b9a757c1 onwards (release v3.0.2 onwards) contains a CWE-125: Out-of-bounds Read vulnerability in 7zip decompression, archive_read_support_format_7zip.c, header_bytes() that can result in a crash (denial of service). |

| CVE | Description |
|----------------------------------|---|
| CVE-2018-6829 | cipher/elgama.c in Libgrypt through 1.8.2, when used to encrypt messages directly, improperly encodes plaintexts, which allows attackers to obtain sensitive information by reading ciphertext data (i.e., it does not have semantic security in face of a ciphertext-only attack). |
| CVE-2018-5883 | Improper Validation of Array Index in WLAN |
| CVE-2018-5863 | Buffer Copy without Checking Size of Input in WLAN |
| CVE-2018-5839 | Improper Access Control in Core |
| CVE-2018-5832 | Use After Free in Camera |
| CVE-2018-5831 | Integer Overflow or Wraparound in Graphics |
| CVE-2018-5407 | Simultaneous Multi-threading (SMT) in processors can enable local users to exploit software vulnerable to timing attacks via a side-channel timing attack on 'port contention'. |
| CVE-2018-3587 | Use After Free in WLAN |
| CVE-2018-3585 | NULL pointer dereference when configuring the actuator in Camera |
| CVE-2018-3581 | Improper Restriction of Operations within the Bounds of a Memory Buffer in WLAN |
| CVE-2018-3576 | Improper Validation of Array Index in WLAN |
| CVE-2018-20843 | In libexpat in Expat before 2.2.7, XML input including XML names that contain a large number of colons could make the XML parser consume a high amount of RAM and CPU resources while processing (enough to be usable for denial-of-service attacks). |
| CVE-2018-20679 | An out of bounds read in udhcp components (consumed by the DHCP server, client, and relay) allows a remote attacker to leak sensitive information from the stack by sending a crafted DHCP message. |
| CVE-2018-13912 | Untrusted Pointer Dereference in Camera |
| CVE-2018-11923 | Potential overflow in wma_stats_event_handler |
| CVE-2018-11897 | Out-of-Bounds read while processing diag event when ssid length is greater than max limit |
| CVE-2018-11869 | Possible buffer overflow in wma_stats_ext_event_handler |
| CVE-2018-11843 | Use-After-Free Issue in WLAN |
| CVE-2018-11842 | Possible Denial of service due to uninitialized data in limSendAssocReqMgmtFrame as part of wlan association |
| CVE-2018-11302 | Buffer Copy Without Checking Size of Input in WLAN |
| CVE-2018-10910 | A bug in Bluez may allow for the Bluetooth Discoverable state being set to on when no Bluetooth agent is registered with the system. |
| CVE-2018-1000880 | libarchive version commit 9693801580c0cf7c70e862d305270a16b52826a7 onwards (release v3.2.0 onwards) contains a CWE-20: Improper Input Validation vulnerability in WARC parser - libarchive/archive_read_support_format_warc.c, _warc_read() that can result in DoS - quasi-infinite run time and disk usage from tiny file. |
| CVE-2018-1000879 | libarchive version commit 379867ecb330b3a952fb7bfa7bffb7bbd5547205 onwards (release v3.3.0 onwards) contains a CWE-476: NULL Pointer Dereference vulnerability in ACL parser - libarchive/archive_acl.c, archive_acl_from_text_l() that can result in Crash/DoS. |
| CVE-2018-1000878 | libarchive version commit 416694915449219d505531b1096384f3237dd6cc onwards (release v3.1.0 onwards) contains a CWE-416: Use After Free vulnerability in RAR decoder - libarchive/archive_read_support_format_rar.c that can result in Crash/DoS - it is unknown if RCE is possible. |
| CVE-2018-1000877 | libarchive version commit 416694915449219d505531b1096384f3237dd6cc onwards (release v3.1.0 onwards) contains a CWE-415: Double Free vulnerability in RAR decoder - libarchive/archive_read_support_format_rar.c, parse_codes(), realloc(rar->lzss.window, new_size) with new_size = 0 that can result in Crash/DoS. |
| CVE-2017-8269 | Information Exposure in Data |

| | | | |
|-------------|---------|-----------|-------|
| Template #: | 4124005 | Revision: | 01.06 |
|-------------|---------|-----------|-------|

| CVE | Description |
|--------------------------------|--|
| CVE-2017-17772 | Set the minsize of SuppChannels IE to 2 |
| CVE-2017-17769 | Possible Information Leak in send_rtac_asm_apr(), send_asm_apr(), send_voice_apr() and send_rtac_afe_apr() |
| CVE-2017-16231 | In PCRE 8.41, after compiling, a pcretest load test PoC produces a crash overflow in the function match() in pcre_exec.c because of a self-recursive call. NOTE: third parties dispute the relevance of this report, noting that there are options that can be used to limit the amount of stack that is used. |
| CVE-2017-15858 | Use After Free in ath9k_tx99_init |
| CVE-2017-15837 | Potential Buffer Over-read for attribute NL80211_PKTPAT_OFFSET |

5.4 Known Issues

This section presents all known issues in this release.

| ID | Title | Description | Impacted Domain |
|----------------------|---|--|-----------------|
| Bugs | | | |
| ECHO-988 | Device fails to enter ULPM | Customer has noticed that occasionally the module will fail to enter ULPM when requested | ULPM |
| ECHO-969 | Crash when upgrading firmware via XMODEM over UART | An "Invalid Port Index" crash is observed when upgrading firmware via XMODEM over UART interface | UART |
| ECHO-962 | USB Selective Suspend crash | After several USB-SS suspend/resume cycles, a crash was observed | USB |
| ECHO-961 | Kernel panic on bootup | One customer has observed a kernel panic on bootup | Linux Stability |
| 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 are not removed after the service is stopped. | Driver |
| ECHO-993 | CMUX command mode | DTR signal does not switch module from data mode to command mode during a data call through DLC port | CMUX |
| 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 |
| ECHO-924 ECHO-975 | Current draw higher than expected when in PSM | ~30% higher than guidance | PSM |
| QT19X06-192 | Device will not enter ULPM/PSM mode if GPIO36/38 is selected as the wakeup source | If GPIOs 36 and 38 are configured as a wakeup source with logic level high as the wakeup trigger, the device is unable to enter PSM or ULPM. The issue doesn't happen when using all other types of wakeup triggers. | PSM |



| ID | Title | Description | Impacted Domain |
|--------------|---|--|-----------------|
| QT19X06-374 | Update MCU firmware to version 002.015 | Includes bug fix: <ul style="list-style-type: none"> MCU-108 – During stress testing of GPIO 38 interrupts, the interrupt may get into a state where it does not respond. | |
| ECHO-672 | RFC 2460 Compliance test case v6LC_1_2_01 failure | The device is currently failing test case v6LC_1_2_01 for IPV6 RFC 2460 compliance due to failure to send a Parameter Problem message during the test. | Data |
| QT19X07-2076 | No Legato Event after an OPEN CHANNEL | No Legato event is reported for STK BIP Open Channel proactive command | Legato |

6 SWI9X06Y Release 12

Release 12 is a major release for WP77xx. This release brings in a new Qualcomm stack, updated Linux kernel minor version, and migration to Yocto 2.5. Each of these improvements provide a significant number of security enhancements. There are also improvements to R2C and FOTA functionality. MCU FW is updated to version 002.013 to solve a stability issue during I2C stress testing. Delta FOTA has been introduced in this release, but the feature has not been validated yet.

6.1 Software Release Description

6.1.1 Release identification

| Component | Revision |
|------------------------------|--|
| Modem Firmware | SWI9X06Y_02.32.02.00 c2e98c jenkins 2019/08/30 07:28:21 |
| Linux Firmware | SWI9X06Y_02.32.02.00 2019-08-30_11:05:02 |
| MCU Firmware | 002.013 (embedded as a binary in the Linux image, not distributed as a separate component) |
| Legato Application Framework | 19.07.0_6ebfa306dc802a91d515da9361145709 |
| Binary Size | 56MB (compressed binaries) |
| IMEI SV | 4 |
| Qualcomm Stack Version | MDM9206.LE.2.0-00173-STD.PROD-1.213823.1 |
| Linux Kernel Version | Linux swi-mdm9x28-wp 3.18.140 #1 PREEMPT Fri Aug 30 10:01:23 UTC 2019 armv7l GNU/Linux |
| Supported H/W | WP7702, WP7700 |

6.1.2 Software Tools Versions

| S/W Tools Name | Version |
|------------------------|------------|
| Windows Driver Package | B4956 |
| Windows SDK | None |
| Skylight | None |
| Linux Drivers | S2.37N2.58 |

| | | | |
|-------------|---------|-----------|-------|
| Template #: | 4124005 | Revision: | 01.06 |
|-------------|---------|-----------|-------|



| S/W Tools Name | Version |
|----------------|--------------|
| Linux SDK | SLQS04.00.21 |

6.1.3 Released Files and Download Processes

| Files | Carrier | Modem Firmware | Config | Linux Distribution | Base Legato System | Comment |
|---|----------------------------|----------------------|-------------|----------------------|--------------------|---------------------------|
| WP7702 Approved | | | | | | |
| WP77xx_Release 12_GENERIC_TM OBILE.exe | GENERIC (T-Mobile) | SWI9X06Y_02.13.02.00 | 001.009_001 | SWI9X06Y_02.32.02.00 | 19.07.0 | T-Mobile USA Approved |
| WP77xx_Release 12_GENERIC_GC F.exe | GENERIC (GCF) | SWI9X06Y_02.32.02.00 | 001.055_000 | SWI9X06Y_02.32.02.00 | 19.07.0 | GCF Approved |
| WP77xx_Release 12_GENERIC_PT CRB.exe | GENERIC (PTCRB) | SWI9X06Y_02.16.06.00 | 001.028_004 | SWI9X06Y_02.32.02.00 | 19.07.0 | PTCRB Approved |
| WP77xx_Release 12_SIERRA.exe | SIERRA | SWI9X06Y_02.32.02.00 | 001.027_000 | SWI9X06Y_02.32.02.00 | 19.07.0 | GCF Approved |
| WP77xx_Release 12_ATT.exe | ATT | SWI9X06Y_02.16.06.00 | 001.026_001 | SWI9X06Y_02.32.02.00 | 19.07.0 | AT&T Approved |
| WP77xx_Release 12_GENERIC_DT .exe | GENERIC (Deutsche Telekom) | SWI9X06Y_02.22.02.00 | 001.041_001 | SWI9X06Y_02.32.02.00 | 19.07.0 | Deutsche Telekom Approved |
| WP77xx_Release 12_VERIZON.exe | VERIZON | SWI9X06Y_02.22.12.00 | 001.042_001 | SWI9X06Y_02.32.02.00 | 19.07.0 | Verizon Approved |
| WP7700 Approved | | | | | | |
| WP77xx_Release 12_GENERIC_GC F.exe | GENERIC (GCF) | SWI9X06Y_02.32.02.00 | 001.055_000 | SWI9X06Y_02.32.02.00 | 19.07.0 | GCF Approved |
| WP77xx_Release 12_GENERIC_PT CRB.exe | GENERIC (PTCRB) | SWI9X06Y_02.16.06.00 | 001.028_004 | SWI9X06Y_02.32.02.00 | 19.07.0 | PTCRB Approved |
| WP77xx_Release 12_SIERRA.exe | SIERRA | SWI9X06Y_02.32.02.00 | 001.027_000 | SWI9X06Y_02.32.02.00 | 19.07.0 | GCF Approved |
| WP77xx_Release 12_ATT.exe | ATT | SWI9X06Y_02.16.06.00 | 001.026_001 | SWI9X06Y_02.32.02.00 | 19.07.0 | AT&T Approved |
| WP77xx_Release 12_VERIZON.exe | VERIZON | SWI9X06Y_02.22.12.00 | 001.042_001 | SWI9X06Y_02.32.02.00 | 19.07.0 | Verizon Approved |
| From: https://source.sierrawireless.com/resources/airprime/software/wp77xx/wp77xx-firmware-release-12 | | | | | | |

| Function | Files |
|---|--|
| Firmware Components | 9999999_9907618_SWI9X06Y_02.13.02.00_00_GENERIC_001.009_001.spk (T-Mobile USA) 9999999_9907618_SWI9X06Y_02.16.06.00_00_GENERIC_001.028_004.spk (PTCRB) 9999999_9907618_SWI9X06Y_02.22.02.00_00_GENERIC_001.041_001.spk (Deutsche Telekom) 9999999_9907618_SWI9X06Y_02.32.02.00_00_GENERIC_001.055_000.spk (GCF) 9999999_9908788_SWI9X06Y_02.32.02.00_00_SIERRA_001.027_000.spk 9999999_9907787_SWI9X06Y_02.16.06.00_00_ATT_001.026_001.spk 9999999_9908088_SWI9X06Y_02.22.12.00_00_VERIZON_001.042_001.spk linux-SWI9X06Y_02.32.02.00.cwe legato-19.07.0.cwe |
| From: https://source.sierrawireless.com/resources/airprime/software/wp77xx/wp77xx-firmware-release-12 | |

| | | | |
|-------------|---------|-----------|-------|
| Template #: | 4124005 | Revision: | 01.06 |
|-------------|---------|-----------|-------|



6.1.4 Available Memory

Flash:

| NAME | PARTITION | ALLOCATION (KB) | IMGSIZE (KB) | USAGE |
|------------------|-----------------|-----------------|--------------|-------|
| LK boot | mtd12 (boot) | 14336 | 8865 | 62% |
| Linux Kernel | mtd13 (system) | 29952 | 23552 | 79% |
| Legato Framework | mtd14 (lefwkro) | 8704 | 6145 | 70% |
| SWIRW | mtd15 (swirw) | 24576 | | |
| USERAPP | mtd16 (userapp) | 133120 | | |

RAM:

104444 kB^{[1][2]}

[1] Value is read from the MemAvailable parameter in /proc/meminfo

[2] Values are for reference only and will vary depending on what services/processes are running at the time of measurement

6.2 Software Changes Description

The WP77xx Release 12 is based on modem and Linux versions SWI9X06Y_02.32.02.00. This release includes all the changes from WP76xx Release 13, with notable / additional changes and features listed below.

| ID | Title | Description | Impacted Domain |
|----------------------|---|--|-----------------|
| Legato | | | |
| Various | Legato 19.07.0 | <p>Legato 19.07.0: https://legato.io/releases</p> <p>Upgrade from 18.09.2 in Release 11.</p> <p>Includes:</p> <ul style="list-style-type: none"> LE-11324 - Failed to set polling timer value by AT command LE-12382 - AVMS reports "WDSI: 15" after FOTA LE-12310 - Module is failed to start AVMS session after recreating new system LE-12309 - AVMS: Fail to synchronize to AVMS server | Legato AF |
| ECHO-712 LE-11902 | AVMS Heartbeat doesn't work for periods >= 4 hr | <p>On some networks including the Sierra Wireless Core network, the network will detach the device after a period of inactivity. Previously, Legato could not handle such a scenario and therefore polling will commonly fail on those networks if it is set to longer than 4 hours.</p> <p>This issue has been fixed since the Legato 19.02 release. For the Sierra Wireless core network, this is expected to be resolved in the future where the timeout will be extended significantly on LPWA APNs.</p> | FOTA |

| | | | |
|-------------|---------|-----------|-------|
| Template #: | 4124005 | Revision: | 01.06 |
|-------------|---------|-----------|-------|

| ID | Title | Description | Impacted Domain |
|--|---|--|-----------------|
| ECHO-757 ECHO-770 | Unable to resume a FOTA download after failure in the middle of a previous download process | In previous releases, Legato does not support resuming a FOTA job if it fails in the middle of a package download. If a FOTA download fails due to events including, but not limited to, device reset, power loss, or AirVantage connection problems, the download will appear to resume but will end up failing. When this happens, the FOTA job must be restarted (rather than resumed). This has been fixed since the Legato 19.02 release. | FOTA |
| ECHO-708 LE-12462 | [VERIZON] Synchronization failed on attempt to retrieve data object of IMSI (lwm2m.10241.0.2) | Legato is unable to read the IMSI from some SIM cards that contain a CSIM application which is listed first, such as some of Verizon's SIM cards. This in turn will cause synchronization failures with the Airvantage server. This has been fixed in 19.07.0. | Connectivity |
| LE-11212 QT19X07-2418 QT19X07-2474 | Current consumption is high when used with a SIM PIN locked SIM card | Fixed an issue when using a locked SIM card, the module will fail to enter sleep mode after SIM is unlocked and synchronized to the network | Low power mode |
| Linux Distribution | | | |
| Various | Upgrade Linux Distro to LXSWI2.5-9.0, based on Yocto 2.5 | Upgrade to LXSWI2.5-9.0 from LXSWI2.2-10.0 (Release 11). New Linux reference now based on Yocto 2.5. | Linux baseline |
| QT19X07-2696 | Modem Daemon crashes when le_mdc_GetDisconnectionReason function has been called | Fixed a crash where modem daemon in Linux will crash when querying the disconnection reason from Legato. | Legato |
| QT19X07-2535 | Unable to build Yocto image with QCA9377_BUILD enabled | User is now able to build with QCA9377 wifi driver enabled. | Yocto |
| MCU FW | | | |
| QT19X06-208 | Update MCU FW to version 002.013 | <p>MCU FW Version has been updated to 002.013 in this release.</p> <p>Includes bug fix:</p> <ul style="list-style-type: none"> MCU-104 / QT19X07-3371 - I2C bus failure occurs when reading ADC2 and entering ULPM <p>In some corner cases with MCU communication, such as reading ADC2 (from MCU) when ULPM mode is requested, an I2C bus failure occurs. The I2C bus failure prevents all future communication with MCU or any other devices on the I2C bus after resuming from ULPM. This issue was fixed in MCU FW 002.013.</p> | MCU FW |
| Modem | | | |
| Core | | | |

| ID | Title | Description | Impacted Domain |
|------------------------------|--|---|--------------------|
| Various | Multiple Qualcomm stack updates to: MDM9206.LE.2.0-00173-STD.PROD-1.213823.1 | Add Qualcomm baseline MDM9206.LE.2.0-00173-STD.PROD-1.213823.1. Includes: <ul style="list-style-type: none"> ECHO-798 - [R2C] SEND SHORT MESSAGE proactive command issue QT19X06-182 - CR 2090010 for interface to access PMIC GPIO input level in MPSS and BOOT QT19X07-3435 – [CMUX] module sends MUX frame with incorrect FCS when frame length is 127 | Qualcomm baseline |
| Protocol/Certification | | | |
| QT19X06-174 | Increase IMEI SV to 4 | The IMEI SV has been increased to 4 in this release. | IMEI SV |
| QT19X07-3487 | Update TS.25 list to April 29, 2019 | Default TS.25 list updated. Non-GSMA PLMNs removed except Test PLMNs. | GCF |
| QT19X07-3355 | Verizon Carrier LWM2M FOTA Support | Support for Verizon Carrier LWM2M FOTA has been added in this release. This feature has not yet been validated on this product yet, and will be tested prior to device lab entry for Verizon MR. | Carrier LWM2M FOTA |
| QMI | | | |
| QT19X07-3512 | Add QMI command to read and write HW Watchdog parameters | Adds interface support for MCU watchdog feature | Stability |
| GNSS | | | |
| QT19X07-3308 QT19X07-2701 | AT!GPSCLRASSIST can't clear GPS Status or Time Info | Fixes various issues with clearing GPS assist data | GNSS |
| QT19X07-3381 | "Unknown" retrieved in GPSLOC resp though GPSTRACK and GPSFIX | Resolves issue with GPS tracking using short interval | GNSS |
| IO | | | |
| QT19X07-3382 QT19X07-3321 | GPIO function NV unexpectedly changed | Fixed the issue where some of the content in NV EXT_GPIO_FUN changed from '10' to '00' after configuration process. | GPIO |
| QT19X07-2672 QT19X07-3264 | GPIO6 is not configurable using +WIOCFG and sysfs | Fixed the issue where GPIO6 cannot be read, written, or configured using +WIOR, +WIOV, and +WIOCFG. | GPIO |
| Security | | | |
| QT19X07-2870 | Possibility of having userapp partition erased | Close the security hole by blocking the userapp updated in bootloader. | Security |
| QT19X07-2946 | A QMI secure file open command returns success even though operation has failed. | Check for NULL file pointer and propagate error from sfs and map to corresponding QMI error. | SFS |
| AT Commands | | | |
| QT19X07-3079 | Add AT command to read and write HW Watchdog parameters | Adds interface support for MCU watchdog feature | Stability |
| QT19X07-3425 | AT!GPSAUTOSTART? value does not match with documentation | Fixes AT!GPSAUTOSTART? parameters to align with documented values | GNSS |
| QT19X07-1739 | !SCACT with invalid state return OK | Resolves issue with AT!SCACT command parameter input validation | Connectivity |



| ID | Title | Description | Impacted Domain |
|-----------------------|--|--|-----------------|
| QT19X07-3432 | AT+COPS=? return wrong long/short alphanumeric <oper> name | Resolves issue with AT+COPS where some PLMN names were displayed incorrectly | 3GPP |
| QT19X07-3815 | AT+COPS? returns "ROGERS ROGERS" | Resolves issue where UE displays registered PLMN name regardless of display condition | 3GPP |
| QT19X07-1062 | URC "+CIEV" is not flushed to the TE with <bfr>=1 | Resolves issue where SMS full indication is not sent to AT terminal | SMS |
| QT19X07-3081 | PDP context authentication configuration | Adds AT+CGAUTH command support for PDP context authentication parameter configuration | Connectivity |
| QT19X07-3545 | Add AT+CSPN to read the service provider name from SIM | Adds support for AT+CSPN command to read Service Provider Name from SIM | GNSS |
| QT19X07-3051 | Xtra data status in GPSXTRASTATUS? always returns Unknown | Resolves issue with GPS XTRA data information not displaying correctly | GNSS |
| QT19X07-3536 | Unknown received when SLR is executed GPS out-of-coverage | Resolves issue with assisted GPS information not displaying correctly when initiated from out-of-coverage | GNSS |
| Factory/Configuration | | | |
| ECHO-799 | Using internal SIM, the APN is lp.swir instead of lp.fota.swir | Sub-PRIs have been added to the Sierra Carrier PRI to allow APNs to be dynamically switched based on the type of Sierra SIM that is being used (embedded vs. external plastic SIM) | Configuration |
| QT19X07-2669 | Private APN setting is lost when switching between carrier PRI | Sub-PRI switching feature is improved with persistence that protect the setting across firmware upgrade and carrier switch. | Configuration |
| QT19X07-2668 | Apply sub-PRI configuration without reset | Able to apply the Sub-PRI configuration on-the-fly without reset. | Configuration |
| QT19X07-3315 | AT!CUSTOM BANDSELEN not persistent over FW upgrades | The setting of AT!CUSTOM="BANDSELEN",1 to enable Antenna Select feature will not stay persistent across a firmware upgrade. This has been fixed now. | NV |
| QT19X07-3483 | Remote NVUP file updates don't work | A bug in the firmware was preventing configuration tools from updating files in the Linux filesystem. This was preventing the update of MCU FW. This issue has been fixed now. | NV |

6.3 Security Corrections/Improvements

| CVE | Description |
|----------------|--|
| CVE-2019-10525 | Stack buffer overflows when receiving segmented SIBs in TD-SCDMA |
| CVE-2019-2296 | Integer Overflow to Buffer Overflow Issue in LTE |
| CVE-2019-10516 | Buffer Over-read Issue in Multi Mode Call processor |
| CVE-2018-13924 | Stack Based Buffer Overflow in MMCP |
| CVE-2018-13911 | Buffer Over-read issue in GNSS XTRA Parser |
| CVE-2018-13902 | Improper Validation of Array Index in GNSS XTRA Parser |
| CVE-2019-2271 | Buffer Over-read in MMCP |
| CVE-2019-2254 | Use of Out-of-range Pointer Offset in GPS |
| CVE-2018-13885 | Information Exposure in MODEM |
| CVE-2019-2289 | Improper Authentication in NAS |

| | | | |
|-------------|---------|-----------|-------|
| Template #: | 4124005 | Revision: | 01.06 |
|-------------|---------|-----------|-------|



| CVE | Description |
|----------------|---|
| CVE-2019-2271 | Improper Validation of Array Index in MMCP |
| CVE-2019-10500 | Incorrect Calculation of Buffer Size in NAS |
| CVE-2019-2303 | Buffer Over-read Issue in GSNDP Module Due to Missing Input Validation |
| CVE-2019-10511 | Improper Validation of Array Index in GSM EDGE Radio Access Network |
| CVE-2019-10487 | Buffer Over-read Issue in Multi-mode Call processor |
| CVE-2019-10485 | Loop With Unreachable Exit Condition in GSM EDGE Radio Access Network |
| CVE-2019-2320 | Possible out of bounds write in a MT SMS/SS Scenario |
| CVE-2019-2335 | Loop with Unreachable Exit Condition in NAS |
| CVE-2019-2337 | Buffer Over-read Issue in NAS |
| CVE-2019-10610 | Buffer Over-read in Modem Data |
| CVE-2019-10554 | Buffer Over-read Issue in Multi Mode Call Processor |
| CVE-2019-10552 | Buffer Over-read Issue in Multi-mode Call Processor |
| CVE-2019-10551 | String Errors in Modem Data |
| CVE-2019-10609 | Improper Validation of Array Index in Modem Data |
| CVE-2019-10593 | Improper Validation of Array Index in Data Modem |
| CVE-2019-10577 | Buffer Over-read Issue in Modem Data |
| CVE-2019-10550 | Buffer Over-read Issue in Modem Data |
| CVE-2018-3570 | Untrusted Pointer Dereference in Core |
| CVE-2018-13917 | Use After Free in HLOS Data |
| CVE-2018-12006 | Information Exposure in Display |
| CVE-2018-11947 | Information Exposure Issue in WLAN |
| CVE-2019-10508 | Buffer Copy Without Checking Size of Input in WLAN |
| CVE-2019-10508 | Buffer Copy Without Checking Size of Input in WLAN |
| CVE-2019-2263 | Use After Free While Reading from Diag Driver |
| CVE-2018-11986 | Buffer Copy Without Checking Size of Input in Camera |
| CVE-2018-13913 | Improper Validation of Array Index in Display |
| CVE-2018-13893 | Untrusted Pointer Dereference in DIAG Services |
| CVE-2018-11894 | PRIMA: Integer Overflow or Wraparound in WLAN |
| CVE-2018-13900 | Use After Free issue in HLOS Data |
| CVE-2018-13892 | Buffer Copy Without Checking Size of Input in WLAN |
| CVE-2018-13925 | Use After Free in Video |
| CVE-2018-9417 | Change Request 2272404 : A-74447444: EoP in Kernel components [2018-07] |
| CVE-2018-12011 | Information Exposure in Core |
| CVE-2018-11902 | Improper Validation of Array Index in WLAN |
| CVE-2018-9422 | A-74250718: EoP in Kernel components [2018-07] |
| CVE-2018-11306 | Information Exposure in BAM drivers |
| CVE-2018-9416 | A-75300370: EoP in Kernel components [2018-07] |

| | | | |
|-------------|---------|-----------|-------|
| Template #: | 4124005 | Revision: | 01.06 |
|-------------|---------|-----------|-------|

| CVE | Description |
|----------------|---|
| CVE-2018-11894 | CLD2.0: Integer Overflow to Buffer Overflow in WLAN |
| CVE-2017-15843 | Double free in msm_bus_floor_vote_context() |
| CVE-2018-11826 | Integer Overflow to Buffer Overflow in WLAN |
| CVE-2018-11276 | Double Free Issue in Kernel |
| CVE-2018-11963 | Buffer Over-read in Camera |
| CVE-2018-12005 | Use After Free in HLOS-Linux |
| CVE-2018-11897 | Out-of-Bounds read while processing diag event when ssid length is greater than max limit |
| CVE-2018-11911 | Permission, privileges and Access Controls in Yocto |
| CVE-2018-11912 | Permissions, Privileges and Access Controls in Yocto |
| CVE-2018-11924 | Integer Overflow to Buffer Overflow in WLAN |
| CVE-2018-12010 | Stack-based Overflow in Core |
| CVE-2017-15850 | (QPSIIR-854/A-62464339) DebugFS entry allows reading of "Always On" Audio Codec WCD9XXX registers |
| CVE-2018-11913 | Permissions, Privileges and Access Controls in Yocto |
| CVE-2018-3574 | Improper Input Validation in Kernel |
| CVE-2018-5905 | Buffer Copy Without Checking Size of Input in DIAG |
| CVE-2018-11984 | Use After Free in Diag Services |
| CVE-2018-3587 | Use After Free in WLAN |
| CVE-2018-11293 | Buffer Over-read in WLAN |
| CVE-2018-11988 | Use After Free in Ecosystem |
| CVE-2018-11301 | Integer Underflow in WLAN |
| CVE-2018-11860 | Buffer Copy Without Checking Size of Input in WLAN |
| CVE-2018-11967 | Permissions, Privileges and Access Controls in DSP Memory |
| CVE-2018-13919 | Use-After-Free issue in IPA Driver while Resetting the Routing Table |
| CVE-2018-11934 | Incorrect Type Conversion or Cast in WLAN |
| CVE-2019-10480 | Buffer Copy Without Checking Size of Input in WLAN Host |
| CVE-2018-11980 | Buffer Copy Without Checking Size of Input in WLAN |
| CVE-2019-2244 | Integer Overflow to Buffer Overflow in Video |
| CVE-2019-2245 | Integer Overflow to Buffer Overflow in Video |
| CVE-2019-2247 | Double Free Issue in Core |
| CVE-2019-2248 | Stack Based Buffer Overflow in Display |
| CVE-2017-8251 | Out of Bounds Array Access in CameraV2 Driver |
| CVE-2019-10557 | Buffer Over-read in WLAN |
| CVE-2019-10557 | Buffer Over-read in WLAN |
| CVE-2019-2306 | Buffer Over-read in Display |
| CVE-2019-2307 | Integer Underflow Issue in WLAN |
| CVE-2018-11955 | CLD2.0: Buffer Over-read in WLAN |



| CVE | Description |
|----------------|---|
| CVE-2018-11955 | PRIMA: Buffer Over-read in WLAN |
| CVE-2019-2299 | Integer Overflow to Buffer Overflow in WLAN HOST |
| CVE-2019-2297 | Integer Overflow to Buffer Overflow in WLAN |
| CVE-2017-17772 | Possible connection failure for some ap |
| CVE-2019-2290 | Use After Free Issue in Camera |
| CVE-2017-15828 | Integer Overflow to Buffer Overflow vulnerability in bootloader |
| CVE-2018-11964 | Permissions, Privilege and Access Controls in Yocto |
| CVE-2018-3573 | Improper Restriction of Operations within the Bounds of a Memory Buffer in Boot |
| CVE-2019-10528 | Use After Free in Diag Services |
| CVE-2019-2298 | Use After Free Issue in Diag Services |
| CVE-2019-2302 | Buffer Copy Without Checking Size of Input in WLAN |
| CVE-2019-2310 | Buffer Over-read Issue in WLAN |
| CVE-2017-17772 | Connection failure with AP using QBSS version 1 IE |
| CVE-2019-2283 | Improper Input Validation in KERNEL |
| CVE-2019-10542 | Buffer Copy Without Checking Size of Input in WLAN HOST |
| CVE-2019-2287 | Use of Out-of-range Pointer Offset in Video |
| CVE-2019-2322 | Integer Overflow to Buffer Overflow Issue in Video |
| CVE-2019-2323 | Improper Input Validation Issue in HLOS |
| CVE-2019-2324 | Improper Validation of Array Index in Audio |
| CVE-2019-2325 | Improper Validation of Array Index in Audio Driver |
| CVE-2019-2326 | Improper Validation of Array Index in Audio Driver |
| CVE-2019-2327 | Buffer Copy Without Checking Size of Input in Video |
| CVE-2019-2328 | Buffer Copy Without Checking Size of Input in Audio Driver |
| CVE-2019-2331 | Integer Overflow or Wraparound Issue in Audio |
| CVE-2019-2332 | Improper Validation of Array Index in Audio |
| CVE-2019-2334 | Null Pointer Dereference Issue in Video |
| CVE-2019-2341 | Buffer Copy Without Checking Size of Input in Audio |
| CVE-2019-10498 | Buffer Copy Without Checking Size of Input in Storage Systems |
| CVE-2014-9940 | regulator: core: Fix regulator_ena_gpio_free not to access pin after freeing |
| CVE-2015-3288 | mm: avoid setting up anonymous pages into file mapping |
| CVE-2015-8955 | arm64: perf: reject groups spanning multiple HW PMUs |
| CVE-2015-8956 | Bluetooth: Fix potential NULL dereference in RFCOMM bind callback |
| CVE-2015-8962 | sg: Fix double-free when drives detach during SG_IO |
| CVE-2015-8963 | perf: Fix race in swevent hash |
| CVE-2015-8964 | tty: Prevent ldisc drivers from re-using stale tty fields |
| CVE-2015-8967 | arm64: make sys_call_table const |
| CVE-2015-9004 | perf: Tighten (and fix) the grouping condition |

| | | | |
|-------------|---------|-----------|-------|
| Template #: | 4124005 | Revision: | 01.06 |
|-------------|---------|-----------|-------|

| CVE | Description |
|----------------|--|
| CVE-2015-9016 | blk-mq: fix race between timeout and freeing request |
| CVE-2016-0758 | KEYS: Fix ASN.1 indefinite length object parsing |
| CVE-2016-10088 | sg_write()/bsg_write() is not fit to be called under KERNEL_DS |
| CVE-2016-10200 | l2tp: fix racy SOCK_ZAPPED flag check in l2tp_ip{,6}_bind() |
| CVE-2016-10208 | ext4: validate s_first_meta_bg at mount time |
| CVE-2016-10229 | udp: properly support MSG_PEEK with truncated buffers |
| CVE-2016-10254 | The allocate_elf function in common.h in elfutils before 0.168 allows remote attackers to cause a denial of service (crash) via a crafted ELF file, which triggers a memory allocation failure. |
| CVE-2016-10255 | The __libelf_set_rawdata_wlock function in elf_getdata.c in elfutils before 0.168 allows remote attackers to cause a denial of service (crash) via a crafted (1) sh_off or (2) sh_size ELF header value, which triggers a memory allocation failure. |
| CVE-2016-10349 | The archive_le32dec function in archive_endian.h in libarchive 3.2.2 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted file. |
| CVE-2016-10350 | The archive_read_format_cab_read_header function in archive_read_support_format_cab.c in libarchive 3.2.2 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted file. |
| CVE-2016-2053 | ASN.1: Fix non-match detection failure on data overrun |
| CVE-2016-2188 | USB: iowarrior: fix NULL-deref at probe |
| CVE-2016-2543 | ALSA: seq: Fix missing NULL check at remove_events ioctl |
| CVE-2016-2544 | ALSA: seq: Fix race at timer setup and close |
| CVE-2016-2546 | ALSA: timer: Fix race among timer ioctls |
| CVE-2016-3189 | Use-after-free vulnerability in bzip2recover in bzip2 1.0.6 allows remote attackers to cause a denial of service (crash) via a crafted bzip2 file, related to block ends set to before the start of the block. |
| CVE-2016-3951 | cdc_ncm: do not call usbnet_link_change from cdc_ncm_bind |
| CVE-2016-4569 | ALSA: timer: Fix leak in SNDRV_TIMER_IOCTL_PARAMS |
| CVE-2016-4578 | ALSA: timer: Fix leak in events via snd_timer_user_ccallback |
| CVE-2016-6354 | Heap-based buffer overflow in the yy_get_next_buffer function in Flex before 2.6.1 might allow context-dependent attackers to cause a denial of service or possibly execute arbitrary code via vectors involving num_to_read. |
| CVE-2016-6786 | perf: Fix event->ctx locking |
| CVE-2016-6787 | perf: Fix event->ctx locking |
| CVE-2016-6828 | tcp: fix use after free in tcp_xmit_retransmit_queue() |
| CVE-2016-7042 | KEYS: Fix short sprintf buffer in /proc/keys show function |
| CVE-2016-7097 | posix_acl: Clear SGID bit when setting file permissions |
| CVE-2016-7425 | scsi: arcmsr: Buffer overflow in arcmsr_iop_message_xfer() |
| CVE-2016-7913 | xc2028: avoid use after free |
| CVE-2016-7915 | HID: core: prevent out-of-bound readings |
| CVE-2016-8405 | fbdev: color map copying bounds checking |
| CVE-2016-8633 | firewire: net: guard against rx buffer overflows |
| CVE-2016-8650 | mpi: Fix NULL ptr dereference in mpi_powm() |

| | | | |
|-------------|---------|-----------|-------|
| Template #: | 4124005 | Revision: | 01.06 |
|-------------|---------|-----------|-------|

| CVE | Description |
|------------------|--|
| CVE-2016-8655 | packet: fix race condition in packet_set_ring |
| CVE-2016-8666 | tunnels: Don't apply GRO to multiple layers of encapsulation. |
| CVE-2016-9083 | vfiio/pci: Fix integer overflows, bitmask check |
| CVE-2016-9084 | vfiio/pci: Fix integer overflows, bitmask check |
| CVE-2016-9120 | staging/android/ion : fix a race condition in the ion driver |
| CVE-2016-9555 | sctp: validate chunk len before actually using it |
| CVE-2016-9604 | KEYS: Disallow keyrings beginning with '.' to be joined as session keyrings |
| CVE-2016-9793 | net: avoid signed overflows for SO_{SND RVC}BUFFORCE |
| CVE-2016-9794 | ALSA: pcm : Call kill_fasync() in stream lock |
| CVE-2017-0627 | media: uvcvideo: Prevent heap overflow when accessing mapped controls |
| CVE-2017-0750 | f2fs: do more integrity verification for superblock |
| CVE-2017-0861 | ALSA: pcm: prevent UAF in snd_pcm_info |
| CVE-2017-1000 | udp: consistently apply ufo or fragmentation |
| CVE-2017-1000111 | packet: fix tp_reserve race in packet_set_ring |
| CVE-2017-1000112 | udp: consistently apply ufo or fragmentation |
| CVE-2017-1000158 | CPython (aka Python) up to 2.7.13 is vulnerable to an integer overflow in the PyString_DecodeEscape function in stringobject.c, resulting in heap-based buffer overflow |
| CVE-2017-1000251 | Bluetooth: Properly check L2CAP config option output buffer length |
| CVE-2017-1000363 | char: lp: fix possible integer overflow in lp_setup() |
| CVE-2017-1000364 | mm: larger stack guard gap, between vmas |
| CVE-2017-1000365 | fs/exec.c: account for argv/envp pointers |
| CVE-2017-1000379 | mm: larger stack guard gap, between vmas |
| CVE-2017-1000380 | ALSA: timer: Fix race between read and ioctl |
| CVE-2017-1000407 | KVM: VMX: remove I/O port 0x80 bypass on Intel hosts |
| CVE-2017-1000410 | Bluetooth: Properly check L2CAP config option output buffer length |
| CVE-2017-10661 | timerfd: Protect the might cancel mechanism proper |
| CVE-2017-10662 | f2fs: sanity check segment count |
| CVE-2017-10663 | f2fs: sanity check checkpoint segno and blkoff |
| CVE-2017-11089 | cfg80211: Define nla_policy for NL80211_ATTR_LOCAL_MESH_POWER_MODE |
| CVE-2017-11176 | mqueue: fix a use-after-free in sys_mq_notify() |
| CVE-2017-11473 | x86/acpi: Prevent out of bound access caused by broken ACPI tables |
| CVE-2017-11600 | xfrm: policy: check policy direction value |
| CVE-2017-12133 | Use-after-free vulnerability in the clntudp_call function in sunrpc/clnt_udp.c in the GNU C Library (aka glibc or libc6) before 2.26 allows remote attackers to have unspecified impact via vectors related to error path. |
| CVE-2017-12146 | driver core: platform: fix race condition with driver_override |
| CVE-2017-12153 | nl80211: check for the required netlink attributes presence |
| CVE-2017-12154 | kvm: nVMX: Don't allow L2 to access the hardware CR8 |

| CVE | Description |
|----------------|---|
| CVE-2017-12190 | fix unbalanced page recounting in bio_map_user_iov |
| CVE-2017-12192 | KEYS: prevent KEYCTL_READ on negative key |
| CVE-2017-12193 | assoc_array: Fix a buggy node-splitting case |
| CVE-2017-12424 | In shadow before 4.5, the newusers tool could be made to manipulate internal data structures in ways unintended by the authors. Malformed input may lead to crashes (with a buffer overflow or other memory corruption) or other unspecified behaviors. This crosses a privilege boundary in, for example, certain web-hosting environments in which a Control Panel allows an unprivileged user account to create subaccounts. |
| CVE-2017-12762 | isdn/i4l: fix buffer overflow |
| CVE-2017-13080 | mac80211: accept key reinstall without changing anything |
| CVE-2017-13168 | scsi: sg: mitigate read/write abuse |
| CVE-2017-13215 | crypto: algif_skcipher - Load TX SG list after waiting |
| CVE-2017-13216 | staging: android: ashmem: fix a race condition in ASHMEM_SET_SIZE ioctl |
| CVE-2017-13305 | KEYS: encrypted: fix buffer overread in valid_master_desc() |
| CVE-2017-13695 | ACPICA: acpi: acpica: fix acpi operand cache leak in nseval.c |
| CVE-2017-14051 | scsi: qla2xxx: Fix an integer overflow in sysfs code |
| CVE-2017-14106 | tcp: initialize rcv_mss to TCP_MIN_MSS instead of 0 |
| CVE-2017-14140 | Sanitize 'move_pages()' permission checks |
| CVE-2017-14156 | video: fbdev: aty: do not leak uninitialized padding in clk to userspace |
| CVE-2017-14166 | libarchive 3.3.2 allows remote attackers to cause a denial of service (xml_data heap-based buffer over-read and application crash) via a crafted xar archive, related to the mishandling of empty strings in the atol8 function in archive_read_support_format_xar.c. |
| CVE-2017-14340 | xfs: XFS_IS_REALTIME_INODE() should be false if no rt device present |
| CVE-2017-14489 | scsi: scsi_transport_iscsi: fix the issue that iscsi_if_rx doesn't parse nlmsg properly |
| CVE-2017-14501 | libarchive 3.3.2 allows remote attackers to cause a denial of service (xml_data heap-based buffer over-read and application crash) via a crafted xar archive, related to the mishandling of empty strings in the atol8 function in archive_read_support_format_xar.c. |
| CVE-2017-14502 | read_header in archive_read_support_format_rar.c in libarchive 3.3.2 suffers from an off-by-one error for UTF-16 names in RAR archives, leading to an out-of-bounds read in archive_read_format_rar_read_header. |
| CVE-2017-14503 | libarchive 3.3.2 suffers from an out-of-bounds read within lha_read_data_none() in archive_read_support_format_lha.c when extracting a specially crafted lha archive, related to lha_crc16. |
| CVE-2017-14991 | scsi: sg: fixup infoleak when using SG_GET_REQUEST_TABLE |
| CVE-2017-15107 | A vulnerability was found in the implementation of DNSSEC in Dnsmasq up to and including 2.78. Wildcard synthesized NSEC records could be improperly interpreted to prove the non-existence of hostnames that actually exist. |
| CVE-2017-15115 | sctp: do not peel off an assoc from one netns to another one |
| CVE-2017-15265 | ALSA: seq: Fix use-after-free at creating a port |
| CVE-2017-15274 | KEYS: fix dereferencing NULL payload with nonzero length |
| CVE-2017-15299 | KEYS: don't let add_key() update an uninstantiated key |
| CVE-2017-15537 | x86/fpu: Don't let userspace set bogus xcomp_bv |
| CVE-2017-15649 | packet: in packet_do_bind, test fanout with bind_lock held |

| CVE | Description |
|----------------|---|
| CVE-2017-15804 | The glob function in glob.c in the GNU C Library (aka glibc or libc6) before 2.27 contains a buffer overflow during unescaping of user names with the ~ operator. |
| CVE-2017-15868 | Bluetooth: bnep: bnep_add_connection() should verify that it's dealing with l2cap socket |
| CVE-2017-15873 | The get_next_block function in archival/libarchive/decompress_bunzip2.c in BusyBox 1.27.2 has an Integer Overflow that may lead to a write access violation. |
| CVE-2017-15874 | archival/libarchive/decompress_unlzma.c in BusyBox 1.27.2 has an Integer Underflow that leads to a read access violation. |
| CVE-2017-16525 | USB: serial: console: fix use-after-free after failed setup |
| CVE-2017-16526 | uwb: properly check kthread_run return value |
| CVE-2017-16527 | ALSA: usb-audio: Kill stray URB at exiting |
| CVE-2017-16529 | ALSA: usb-audio: Check out-of-bounds access by corrupted buffer descriptor |
| CVE-2017-16530 | USB: uas: fix bug in handling of alternate settings |
| CVE-2017-16531 | USB: fix out-of-bounds in usb_set_configuration |
| CVE-2017-16532 | usb: usbtest: fix NULL pointer dereference |
| CVE-2017-16533 | HID: usbhid: fix out-of-bounds bug |
| CVE-2017-16535 | USB: core: fix out-of-bounds access bug in usb_get_bos_descriptor() |
| CVE-2017-16537 | media: imon: Fix null-ptr-deref in imon_probe |
| CVE-2017-16538 | media: dvb-usb-v2: lmedm04: Improve logic checking of warm start |
| CVE-2017-16544 | In the add_match function in libbb/lineedit.c in BusyBox through 1.27.2, the tab autocomplete feature of the shell, used to get a list of filenames in a directory, does not sanitize filenames and results in executing any escape sequence in the terminal. This could potentially result in code execution, arbitrary file writes, or other attacks. |
| CVE-2017-16643 | Input: gtco - fix potential out-of-bound access |
| CVE-2017-16645 | Input: ims-psu - check if CDC union descriptor is sane |
| CVE-2017-16646 | media: dib0700: fix invalid dvb_detach argument |
| CVE-2017-16911 | usbip: prevent vhci_hcd driver from leaking a socket pointer address |
| CVE-2017-16912 | usbip: fix stub_rx: get_pipe() to validate endpoint number |
| CVE-2017-16913 | usbip: fix stub_rx: harden CMD_SUBMIT path to handle malicious input |
| CVE-2017-16914 | usbip: fix stub_send_ret_submit() vulnerability to null transfer_buffer |
| CVE-2017-16939 | ipsec: Fix aborted xfrm policy dump crash |
| CVE-2017-17448 | netfilter: nfnetlink_cthelper: Add missing permission checks |
| CVE-2017-17449 | netlink: Add netns check on taps |
| CVE-2017-17450 | netfilter: xt_osf: Add missing permission checks |
| CVE-2017-17558 | USB: core: prevent malicious bNumInterfaces overflow |
| CVE-2017-17805 | crypto: salsa20 - fix blkcipher_walk API usage |
| CVE-2017-17806 | crypto: hmac - require that the underlying hash algorithm is unkeyed |
| CVE-2017-17807 | KEYS: add missing permission check for request_key() destination |
| CVE-2017-17975 | media: usbtv: prevent double free in error case |
| CVE-2017-18017 | netfilter: xt_TCPMSS: add more sanity tests on tcp->doff |

| CVE | Description |
|----------------|--|
| CVE-2017-18018 | In GNU Coreutils through 8.29, chown-core.c in chown and chgrp does not prevent replacement of a plain file with a symlink during use of the POSIX "-R -L" options, which allows local users to modify the ownership of arbitrary files by leveraging a race condition. |
| CVE-2017-18079 | Input: i8042 - fix crash at boot time |
| CVE-2017-18203 | dm: fix race between dm_get_from_kobject() and __dm_destroy() |
| CVE-2017-18204 | ocfs2: should wait dio before inode lock in ocfs2_setattr() |
| CVE-2017-18208 | mm/madvise.c: fix madvise() infinite loop under special circumstances |
| CVE-2017-18221 | mlock: fix mlock count can not decrease in race condition |
| CVE-2017-18255 | perf/core: Fix the perf_cpu_time_max_percent check |
| CVE-2017-18269 | An SSE2-optimized memmove implementation for i386 in sysdeps/i386/i686/multiarch/memcpy-sse2-unaligned.S in the GNU C Library (aka glibc or libc6) 2.21 through 2.27 does not correctly perform the overlapping memory check if the source memory range spans the middle of the address space, resulting in corrupt data being produced by the copy operation. This may disclose information to context-dependent attackers, or result in a denial of service, or, possibly, code execution. |
| CVE-2017-18270 | KEYS: prevent creating a different user's keyrings |
| CVE-2017-18344 | posix-timer: Properly check sigevent->sigev_notify |
| CVE-2017-18360 | USB: serial: io_ti: fix div-by-zero in set_termios |
| CVE-2017-18551 | i2c: core-smbus: prevent stack corruption on read I2C_BLOCK_DATA |
| CVE-2017-18595 | tracing: Fix possible double free on failure of allocating trace buffer |
| CVE-2017-2596 | kvm: fix page struct leak in handle_vmon |
| CVE-2017-2618 | selinux: fix off-by-one in setprocatr |
| CVE-2017-2636 | tty: n_hdlc: get rid of racy n_hdlc.tbuf |
| CVE-2017-2671 | ping: implement proper locking |
| CVE-2017-5601 | An error in the lha_read_file_header_1() function (archive_read_support_format_lha.c) in libarchive 3.2.2 allows remote attackers to trigger an out-of-bounds read memory access and subsequently cause a crash via a specially crafted archive. |
| CVE-2017-5897 | ip6_gre: fix ip6gre_err() invalid reads |
| CVE-2017-5970 | ipv4: keep skb->dst around in presence of IP options |
| CVE-2017-5986 | sctp: avoid BUG_ON on sctp_wait_for_sndbuf |
| CVE-2017-6001 | perf/core: Fix concurrent sys_perf_event_open() vs. 'move_group' race |
| CVE-2017-6074 | dccp: fix freeing skb too early for IPV6_RECVPKTINFO |
| CVE-2017-6214 | tcp: avoid infinite loop in tcp_splice_read() |
| CVE-2017-6345 | net/lc: avoid BUG_ON() in skb_orphan() |
| CVE-2017-6353 | sctp: deny peeloff operation on asocs with threads sleeping on it |
| CVE-2017-7184 | xfrm_user: validate XFRM_MSG_NEWAE XFRMA_REPLAY_ESN_VAL replay_window |
| CVE-2017-7187 | scsi: sg: check length passed to SG_NEXT_CMD_LEN |
| CVE-2017-7261 | drm/vmwgfx: NULL pointer dereference in vmw_surface_define_ioctl() |
| CVE-2017-7294 | drm/vmwgfx: fix integer overflow in vmw_surface_define_ioctl() |
| CVE-2017-7308 | net/packet: fix overflow in check for priv area size |
| CVE-2017-7346 | drm/vmwgfx: limit the number of mip levels in vmw_gb_surface_define_ioctl() |

| | | | |
|-------------|---------|-----------|-------|
| Template #: | 4124005 | Revision: | 01.06 |
|-------------|---------|-----------|-------|

| CVE | Description |
|------------------|--|
| CVE-2017-7472 | KEYS: fix keyctl_set_reqkey_keyring() to not leak thread keyrings |
| CVE-2017-7482 | rxrpc: Fix several cases where a padded len isn't checked in ticket decode |
| CVE-2017-7487 | ipx: call ipxif_put() in ioctl error path |
| CVE-2017-7533 | dentry name snapshots |
| CVE-2017-7541 | brcmfmac: fix possible buffer overflow in brcmf_cfg80211_mgmt_tx() |
| CVE-2017-7542 | ipv6: avoid overflow of offset in ip6_find_1stfragopt |
| CVE-2017-7616 | mm/mempolicy.c: fix error handling in set_mempolicy and mbind. |
| CVE-2017-7618 | crypto: ahash - Fix EINPROGRESS notification callback |
| CVE-2017-7645 | nfsd: check for oversized NFSv2/v3 arguments |
| CVE-2017-7889 | mm: Tighten x86 /dev/mem with zeroing reads |
| CVE-2017-8064 | dvb-usb-v2: avoid use-after-free |
| CVE-2017-8824 | dccp:CVE-2017-8824: use-after-free in DCCP code |
| CVE-2017-8890 | dccp/tcp: do not inherit mc_list from parent |
| CVE-2017-8924 | USB: serial: io_ti: fix information leak in completion handler |
| CVE-2017-8925 | USB: serial: omninet: fix reference leaks at open |
| CVE-2017-9074 | ipv6: Prevent overrun when parsing v6 header options |
| CVE-2017-9075 | sctp: do not inherit ipv6_{mc ac fl}_list from parent |
| CVE-2017-9076 | ipv6/dccp: do not inherit ipv6_mc_list from parent |
| CVE-2017-9077 | ipv6/dccp: do not inherit ipv6_mc_list from parent |
| CVE-2017-9242 | ipv6: fix out of bound writes in __ip6_append_data() |
| CVE-2017-9725 | mm: cma: fix incorrect type conversion for size during dma allocation |
| CVE-2017-9984 | ALSA: msnd: Optimize / harden DSP and MIDI loops |
| CVE-2017-9985 | ALSA: msnd: Optimize / harden DSP and MIDI loops |
| CVE-2018-0495 | Libcrypt before 1.7.10 and 1.8.x before 1.8.3 allows a memory-cache side-channel attack on ECDSA signatures that can be mitigated through the use of blinding during the signing process in the _gcry_ecc_ecdsa_sign function in cipher/ecc-ecdsa.c, aka the Return Of the Hidden Number Problem or ROHNP. To discover an ECDSA key, the attacker needs access to either the local machine or a different virtual machine on the same physical host. |
| CVE-2018-0734 | The OpenSSL DSA signature algorithm has been shown to be vulnerable to a timing side channel attack. An attacker could use variations in the signing algorithm to recover the private key. Fixed in OpenSSL 1.1.1a (Affected 1.1.1). Fixed in OpenSSL 1.1.0j (Affected 1.1.0-1.1.0i). Fixed in OpenSSL 1.0.2q (Affected 1.0.2-1.0.2p). |
| CVE-2018-0739 | Constructed ASN.1 types with a recursive definition (such as can be found in PKCS7) could eventually exceed the stack given malicious input with excessive recursion. This could result in a Denial Of Service attack. There are no such structures used within SSL/TLS that come from untrusted sources so this is considered safe. Fixed in OpenSSL 1.1.0h (Affected 1.1.0-1.1.0g). Fixed in OpenSSL 1.0.2o (Affected 1.0.2b-1.0.2n). |
| CVE-2018-1000001 | In glibc 2.26 and earlier there is confusion in the usage of getcwd() by realpath() which can be used to write before the destination buffer leading to a buffer underflow and potential code execution. |
| CVE-2018-1000004 | ALSA: seq: Make ioctls race-free |
| CVE-2018-1000030 | Python 2.7.14 is vulnerable to a Heap-Buffer-Overflow as well as a Heap-Use-After-Free. |

| CVE | Description |
|------------------|--|
| CVE-2018-1000120 | A buffer overflow exists in curl 7.12.3 to and including curl 7.58.0 in the FTP URL handling that allows an attacker to cause a denial of service or worse. |
| CVE-2018-1000121 | A NULL pointer dereference exists in curl 7.21.0 to and including curl 7.58.0 in the LDAP code that allows an attacker to cause a denial of service |
| CVE-2018-1000122 | A buffer over-read exists in curl 7.20.0 to and including curl 7.58.0 in the RTSP+RTP handling code that allows an attacker to cause a denial of service or information leakage |
| CVE-2018-1000199 | perf/hwbp: Simplify the perf-hwbp code, fix documentation |
| CVE-2018-1000204 | scsi: sg: allocate with __GFP_ZERO in sg_build_indirect() |
| CVE-2018-10021 | scsi: libsas: defer ata device eh commands to libata |
| CVE-2018-10087 | kernel/exit.c: avoid undefined behaviour when calling wait4() |
| CVE-2018-10124 | kernel/signal.c: avoid undefined behaviour in kill_something_info |
| CVE-2018-10372 | process_cu_tu_index in dwarf.c in GNU Binutils 2.30 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted binary file, as demonstrated by readelf. |
| CVE-2018-10373 | concat_filename in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted binary file, as demonstrated by nm-new. |
| CVE-2018-10534 | The _bfd_XX_bfd_copy_private_bfd_data_common function in peXXigen.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, processes a negative Data Directory size with an unbounded loop that increases the value of (external_IMAGE_DEBUG_DIRECTORY) *edd so that the address exceeds its own memory region, resulting in an out-of-bounds memory write, as demonstrated by objcopy copying private info with _bfd_pex64_bfd_copy_private_bfd_data_common in pex64igen.c. |
| CVE-2018-10535 | The ignore_section_sym function in elf.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, does not validate the output_section pointer in the case of a symtab entry with a "SECTION" type that has a "0" value, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted file, as demonstrated by objcopy. |
| CVE-2018-1060 | python before versions 2.7.15, 3.4.9, 3.5.6rc1, 3.6.5rc1 and 3.7.0 is vulnerable to catastrophic backtracking in pop3lib's apop() method. An attacker could use this flaw to cause denial of service. |
| CVE-2018-1061 | python before versions 2.7.15, 3.4.9, 3.5.6rc1, 3.6.5rc1 and 3.7.0 is vulnerable to catastrophic backtracking in the difflib.IS_LINE_JUNK method. An attacker could use this flaw to cause denial of service. |
| CVE-2018-10675 | mm/mempolicy: fix use after free when calling get_mempolicy |
| CVE-2018-1068 | netfilter: ebttables: CONFIG_COMPAT: don't trust userland offsets |
| CVE-2018-1087 | kvm/x86: fix icebp instruction handling |
| CVE-2018-10876 | ext4: only look at the bg_flags field if it is valid |
| CVE-2018-10877 | ext4: verify the depth of extent tree in ext4_find_extent() |
| CVE-2018-10878 | ext4: always check block group bounds in ext4_init_block_bitmap() |
| CVE-2018-10879 | ext4: make sure bitmaps and the inode table don't overlap with bg descriptors |
| CVE-2018-10880 | ext4: never move the system.data xattr out of the inode body |
| CVE-2018-10881 | ext4: clear i_data in ext4_inode_info when removing inline data |
| CVE-2018-10882 | ext4: add more inode number paranoia checks |
| CVE-2018-10883 | jbd2: don't mark block as modified if the handle is out of credits |
| CVE-2018-10902 | ALSA: rawmidi: Change resized buffers atomically |

| | | | |
|-------------|---------|-----------|-------|
| Template #: | 4124005 | Revision: | 01.06 |
|-------------|---------|-----------|-------|

| CVE | Description |
|----------------|---|
| CVE-2018-1092 | ext4: fail ext4_iget for root directory if unallocated |
| CVE-2018-1093 | ext4: add validity checks for bitmap block numbers |
| CVE-2018-10940 | cdrom: information leak in cdrom_ioctl_media_changed() |
| CVE-2018-11236 | stdlib/canonicalize.c in the GNU C Library (aka glibc or libc6) 2.27 and earlier, when processing very long pathname arguments to the realpath function, could encounter an integer overflow on 32-bit architectures, leading to a stack-based buffer overflow and, potentially, arbitrary code execution. |
| CVE-2018-11237 | An AVX-512-optimized implementation of the memcpy function in the GNU C Library (aka glibc or libc6) 2.27 and earlier may write data beyond the target buffer, leading to a buffer overflow in __memcpy_avx512_no_vzeroupper. |
| CVE-2018-1130 | dccp: check sk for closed state in dccp_sendmsg() |
| CVE-2018-12233 | jfs: Fix inconsistency between memory allocation and ea_buf->max_size |
| CVE-2018-12896 | posix-timers: Sanitize overrun handling |
| CVE-2018-13053 | alarmtimer: Prevent overflow for relative nanosleep |
| CVE-2018-13405 | Fix up non-directory creation in SGID directories |
| CVE-2018-13406 | video: uvesafb: Fix integer overflow in allocation |
| CVE-2018-13785 | In libpng 1.6.34, a wrong calculation of row_factor in the png_check_chunk_length function (pngutil.c) may trigger an integer overflow and resultant divide-by-zero while processing a crafted PNG file, leading to a denial of service. |
| CVE-2018-14609 | btrfs: relocation: Only remove reloc rb_trees if reloc control has been initialized |
| CVE-2018-14618 | curl before version 7.61.1 is vulnerable to a buffer overrun in the NTLM authentication code. The internal function Curl_ntlm_core_mk_nt_hash multiplies the length of the password by two (SUM) to figure out how large temporary storage area to allocate from the heap. The length value is then subsequently used to iterate over the password and generate output into the allocated storage buffer. On systems with a 32 bit size_t, the math to calculate SUM triggers an integer overflow when the password length exceeds 2GB (2^31 bytes). This integer overflow usually causes a very small buffer to actually get allocated instead of the intended very huge one, making the use of that buffer end up in a heap buffer overflow. (This bug is almost identical to CVE-2017-8816.) |
| CVE-2018-14633 | scsi: target: iscsi: Use hex2bin instead of a re-implementation |
| CVE-2018-14634 | exec: Limit arg stack to at most 75% of _STK_LIM |
| CVE-2018-14734 | infiniband: fix a possible use-after-free bug |
| CVE-2018-16276 | USB: yurex: fix out-of-bounds uaccess in read handler |
| CVE-2018-16658 | cdrom: Fix info leak/OOB read in cdrom_ioctl_drive_status |
| CVE-2018-16839 | Curl versions 7.33.0 through 7.61.1 are vulnerable to a buffer overrun in the SASL authentication code that may lead to denial of service. |
| CVE-2018-16840 | A heap use-after-free flaw was found in curl versions from 7.59.0 through 7.61.1 in the code related to closing an easy handle. When closing and cleaning up an 'easy' handle in the `Curl_close()` function, the library code first frees a struct (without nulling the pointer) and might then subsequently erroneously write to a struct field within that already freed struct |
| CVE-2018-16842 | Curl versions 7.14.1 through 7.61.1 are vulnerable to a heap-based buffer over-read in the tool_msgs.c:voutf() function that may result in information exposure and denial of service. |
| CVE-2018-16862 | mm: cleancache: fix corruption on missed inode invalidation |
| CVE-2018-16884 | sunrpc: use-after-free in svc_process_common() |

| CVE | Description |
|----------------|--|
| CVE-2018-16890 | libcurl versions from 7.36.0 to before 7.64.0 is vulnerable to a heap buffer out-of-bounds read. The function handling incoming NTLM type-2 messages ('lib/vauth/ntlm.c:ntlm_decode_type2_target') does not validate incoming data correctly and is subject to an integer overflow vulnerability. Using that overflow, a malicious or broken NTLM server could trick libcurl to accept a bad length + offset combination that would lead to a buffer read out-of-bounds. |
| CVE-2018-17182 | mm: get rid of vmacache_flush_all() entirely |
| CVE-2018-17972 | proc: restrict kernel stack dumps to root |
| CVE-2018-18021 | arm64: KVM: Tighten guest core register access from userspace |
| CVE-2018-18281 | mremap: properly flush TLB before releasing the page |
| CVE-2018-18386 | n_tty: fix EXTPROC vs ICANON interaction with TIOCINQ (aka FIONREAD) |
| CVE-2018-18710 | cdrom: fix improper type cast, which can lead to information leak. |
| CVE-2018-19985 | USB: hso: Fix OOB memory access in hso_probe/hso_get_config_data |
| CVE-2018-20169 | USB: check usb_get_extra_descriptor for proper size |
| CVE-2018-20511 | net/appletalk: fix minor pointer leak to userspace in SIOCFINDIPDDPRT |
| CVE-2018-20836 | scsi: libsas: fix a race condition when smp task timeout |
| CVE-2018-5332 | RDS: Heap OOB write in rds_message_alloc_sgs() |
| CVE-2018-5333 | RDS: null pointer dereference in rds_atomic_free_op |
| CVE-2018-5344 | loop: fix concurrent lo_open/lo_release |
| CVE-2018-5750 | ACPI: sbshc: remove raw pointer from printk() message |
| CVE-2018-5803 | sctp: verify size of a new chunk in _sctp_make_chunk() |
| CVE-2018-5814 | usbip: usbip_host: fix NULL-ptr deref and use-after-free errors |
| CVE-2018-5848 | wil6210: missing length check in wmi_set_ie |
| CVE-2018-6412 | fbdev: Fixing arbitrary kernel leak in case FBIOGETCMAP_SPARC in sbusfb_ioctl_helper(). |
| CVE-2018-6485 | An integer overflow in the implementation of the posix_memalign in memalign functions in the GNU C Library (aka glibc or libc6) 2.26 and earlier could cause these functions to return a pointer to a heap area that is too small, potentially leading to heap corruption. |
| CVE-2018-6554 | staging: irda: remove the irda network stack and drivers |
| CVE-2018-6555 | staging: irda: remove the irda network stack and drivers |
| CVE-2018-6759 | The bfd_get_debug_link_info_1 function in opncls.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, has an unchecked strlen operation. Remote attackers could leverage this vulnerability to cause a denial of service (segmentation fault) via a crafted ELF file |
| CVE-2018-6797 | An issue was discovered in Perl 5.18 through 5.26. A crafted regular expression can cause a heap-based buffer overflow, with control over the bytes written. |
| CVE-2018-6798 | An issue was discovered in Perl 5.22 through 5.26. Matching a crafted locale dependent regular expression can cause a heap-based buffer over-read and potentially information disclosure. |
| CVE-2018-6872 | The elf_parse_notes function in elf.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, allows remote attackers to cause a denial of service (out-of-bounds read and segmentation violation) via a note with a large alignment. |
| CVE-2018-6913 | Heap-based buffer overflow in the pack function in Perl before 5.26.2 allows context-dependent attackers to execute arbitrary code via a large item count. |
| CVE-2018-6927 | futex: Prevent overflow by strengthen input validation |

| | | | |
|-------------|---------|-----------|-------|
| Template #: | 4124005 | Revision: | 01.06 |
|-------------|---------|-----------|-------|

| CVE | Description |
|----------------|---|
| CVE-2018-7191 | tun: call dev_get_valid_name() before register_netdevice() |
| CVE-2018-7208 | In the coff_pointerize_aux function in coffgen.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, an index is not validated, which allows remote attackers to cause a denial of service (segmentation fault) or possibly have unspecified other impact via a crafted file, as demonstrated by objcopy of a COFF object. |
| CVE-2018-7492 | rds: Fix NULL pointer dereference in __rds_rdma_map |
| CVE-2018-7566 | ALSA: seq: Fix racy pool initializations |
| CVE-2018-7568 | The parse_die function in dwarf1.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, allows remote attackers to cause a denial of service (integer overflow and application crash) via an ELF file with corrupt dwarf1 debug information, as demonstrated by nm. |
| CVE-2018-7569 | dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, allows remote attackers to cause a denial of service (integer underflow or overflow, and application crash) via an ELF file with a corrupt DWARF FORM block, as demonstrated by nm. |
| CVE-2018-7642 | The swap_std_reloc_in function in aoutx.h in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, allows remote attackers to cause a denial of service (aout_32_swap_std_reloc_out NULL pointer dereference and application crash) via a crafted ELF file, as demonstrated by objcopy. |
| CVE-2018-7643 | The display_debug_ranges function in dwarf.c in GNU Binutils 2.30 allows remote attackers to cause a denial of service (integer overflow and application crash) or possibly have unspecified other impact via a crafted ELF file, as demonstrated by objdump. |
| CVE-2018-7738 | In util-linux before 2.32-rc1, bash-completion/umount allows local users to gain privileges by embedding shell commands in a mountpoint name, which is mishandled during a umount command (within Bash) by a different user, as demonstrated by logging in as root and entering umount followed by a tab character for autocompletion. |
| CVE-2018-7755 | floppy: Do not copy a kernel pointer to user memory in FDGETPRM ioctl |
| CVE-2018-7757 | scsi: libsas: fix memory leak in sas_smp_get_phy_events() |
| CVE-2018-7995 | x86/MCE: Serialize sysfs changes |
| CVE-2018-8740 | In SQLite through 3.22.0, databases whose schema is corrupted using a CREATE TABLE AS statement could cause a NULL pointer dereference, related to build.c and prepare.c. |
| CVE-2018-8781 | drm: udl: Properly check framebuffer mmap offsets |
| CVE-2018-8822 | staging: ncpfs: memory corruption in ncp_read_kernel() |
| CVE-2018-8945 | The bfd_section_from_shdr function in elf.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, allows remote attackers to cause a denial of service (segmentation fault) via a large attribute section. |
| CVE-2018-9363 | Bluetooth: hidp: buffer overflow in hidp_process_report |
| CVE-2018-9422 | futex: Remove requirement for lock_page() in get_futex_key() |
| CVE-2018-9516 | HID: debug: check length before copy_to_user() |
| CVE-2018-9518 | NFC: llcp: Limit size of SDP URI |
| CVE-2018-9568 | net: Set sk_prot_creator when cloning sockets to the right proto |
| CVE-2019-10142 | drivers/virt/fsl_hypervisor.c: prevent integer overflow in ioctl |
| CVE-2019-10639 | netns: provide pure entropy for net_hash_mix() |
| CVE-2019-11190 | binfmt_elf: switch to new creds when switching to new mm |
| CVE-2019-11486 | tty: mark Siemens R3964 line discipline as BROKEN |
| CVE-2019-11810 | scsi: megaraid_sas: return error when create DMA pool failed |

| | | | |
|-------------|---------|-----------|-------|
| Template #: | 4124005 | Revision: | 01.06 |
|-------------|---------|-----------|-------|

| CVE | Description |
|----------------|--|
| CVE-2019-11884 | Bluetooth: hidp: fix buffer overflow |
| CVE-2019-12818 | net: nfc: Fix NULL dereference on nfc_llcp_build_tlv fails |
| CVE-2019-12819 | mdio_bus: Fix use-after-free on device_register fails |
| CVE-2019-15214 | ALSA: core: Fix card races between register and disconnect |
| CVE-2019-15216 | USB: yurex: Fix protection fault after device removal |
| CVE-2019-15292 | appletalk: Fix use-after-free in atalk_proc_exit |
| CVE-2019-1559 | If an application encounters a fatal protocol error and then calls SSL_shutdown() twice (once to send a close_notify, and once to receive one) then OpenSSL can respond differently to the calling application if a 0 byte record is received with invalid padding compared to if a 0 byte record is received with an invalid MAC. If the application then behaves differently based on that in a way that is detectable to the remote peer, then this amounts to a padding oracle that could be used to decrypt data. In order for this to be exploitable "non-stitched" ciphersuites must be in use. Stitched ciphersuites are optimised implementations of certain commonly used ciphersuites. Also the application must call SSL_shutdown() twice even if a protocol error has occurred (applications should not do this but some do anyway). Fixed in OpenSSL 1.0.2r (Affected 1.0.2-1.0.2q). |
| CVE-2019-15916 | net-sysfs: Fix mem leak in netdev_register_kobject |
| CVE-2019-15927 | ALSA: usb-audio: Avoid access before bLength check in build_audio_procunit() |
| CVE-2019-2101 | media: uvcvideo: Fix 'type' check leading to overflow |
| CVE-2019-3459 | Bluetooth: Verify that l2cap_get_conf_opt provides large enough buffer |
| CVE-2019-3460 | Bluetooth: Check L2CAP option sizes returned from l2cap_get_conf_opt |
| CVE-2019-3701 | can: gw: ensure DLC boundaries after CAN frame modification |
| CVE-2019-3822 | libcurl versions from 7.36.0 to before 7.64.0 are vulnerable to a stack-based buffer overflow. The function creating an outgoing NTLM type-3 header ('lib/vauth/ntlm.c: Curl_auth_create_ntlm_type3_message()'), generates the request HTTP header contents based on previously received data. The check that exists to prevent the local buffer from getting overflowed is implemented wrongly (using unsigned math) and as such it does not prevent the overflow from happening. This output data can grow larger than the local buffer if very large 'nt response' data is extracted from a previous NTLMv2 header provided by the malicious or broken HTTP server. Such a 'large value' needs to be around 1000 bytes or more. The actual payload data copied to the target buffer comes from the NTLMv2 type-2 response header. |
| CVE-2019-3823 | libcurl versions from 7.34.0 to before 7.64.0 are vulnerable to a heap out-of-bounds read in the code handling the end-of-response for SMTP. If the buffer passed to 'smtp_endofresp()' isn't NUL terminated and contains no character ending the parsed number, and 'len' is set to 5, then the 'strtol()' call reads beyond the allocated buffer. The read contents will not be returned to the caller. |
| CVE-2019-6133 | fork: record start_time late |
| CVE-2019-6974 | kvm: fix kvm_ioct_create_device() reference counting (CVE-2019-6974) |
| CVE-2019-7221 | KVM: nVMX: unconditionally cancel preemption timer in free_nested (CVE-2019-7221) |
| CVE-2019-7222 | KVM: x86: work around leak of uninitialized stack contents (CVE-2019-7222) |
| CVE-2019-9213 | mm: enforce min addr even if capable() in expand_downwards() |
| CVE-2019-9454 | i2c: core-smbus: prevent stack corruption on read I2C_BLOCK_DATA |
| CVE-2019-9456 | usb: usbmon: Read text within supplied buffer size |
| CVE-2019-9457 | exec: Limit arg stack to at most 75% of _STK_LIM |
| CVE-2019-9458 | media: v4l: event: Prevent freeing event subscriptions while accessed |

6.4 Known Issues

This section presents all known issues in this release.

| ID | Title | Description | Impacted Domain |
|--------------|--|--|-----------------|
| Bugs | | | |
| 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 are not removed after the service is 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 |
| QT19X06-192 | Device will not enter ULPM/PSM mode if GPIO36/38 is selected as the wakeup source | If GPIOs 36 and 38 are configured as a wakeup source with logic level high as the wakeup trigger, the device is unable to enter PSM or ULPM. The issue doesn't happen when using all other types of wakeup triggers. | PSM |
| LE-11753 | Location - Legato le_posCtrl_Request() returning null if GPS already started | If the GNSS engine is configured to start a tracking session automatically upon boot up (AT!GPSAUTOSTART=1), the Legato positioning service internal state will become out of sync with the modem and unable to start a GNSS fix. As a workaround, customers can configure the AT!GPSAUTOSTART setting to Enable only on NMEA open (2) or Disabled (0). | GNSS |
| QT19X07-4262 | Invalid buffer access in idsfashclearwritebuf() causing crash during FOTA download | Occasionally, an invalid buffer access can cause the device to crash during a FOTA update. The FOTA update can still complete successfully after the device resets from the crash. This issue will be fixed in a later release. | FOTA |
| QT19X06-33 | Connectivity Interruption | In lab testing, a scenario has been occasionally observed where connectivity is interrupted every three minutes when using the Sierra Wireless SIM. This issue has not been seen in field testing. A corrective plan is currently ongoing, get in touch with your Sierra Wireless representative for latest update | Connectivity |
| ECHO-672 | RFC 2460 Compliance test case v6LC_1_2_01 failure | The device is currently failing test case v6LC_1_2_01 for IPV6 RFC 2460 compliance due to failure to send a Parameter Problem message during the test. | Data |
| QT19X07-2272 | Periodic high current draw when testing EDRX/DRX with HSIC Enabled | Periodic high current draw is seen when testing EDRX/DRX with HSIC Enabled. Every 3.5 mins, there will be a period of 1.5 mins where the device will wake up and consume around 35mA of current. | System |



| ID | Title | Description | Impacted Domain |
|--------------|---|--|-----------------|
| QT19X07-2195 | SNTP Client unable to use existing connection | Unlike the WPx5, the WP76/77 SNTP client must open a new connection, which is more visible and could have undesirable consequences. Therefore for WP76 the feature is off by default so the user would need to enable it explicitly to get the benefit. This can be done via QMI/Legato, but because it is a AT!CUSTOM feature, a level 2 password is required to enable it via AT | FOTA/Other |
| QT19X07-2186 | Setting identical profile AUTH params forces LTE re-attach with SINGLEAPNSWITCH | With SINGLEAPNSWITCH feature enabled, Legato cm data connect always fails on LTE with Legato 18.05.1 or older | Legato |
| QT19X07-2076 | No Legato Event after an OPEN CHANNEL | No Legato event is reported for STK BIP Open Channel proactive command | Legato |
| QT19X07-1928 | The eth0 address is erased when Wifi chip is inserted after reboot | eth0 address is erased when Wifi chip is inserted after reboot | Driver |

7 SWI9X06Y Release 11

Release 11 is a major release for WP77xx that has achieved FOTA, Connectivity Ready, and AV Ready status. This release includes new features and milestones such as Carrier LWM2M, Brazil Anatel IPV6 Regulatory Conformance support, Deutsche Telekom certification, and is the final candidate for Verizon carrier approval. The same carrier and industrial certifications obtained in Release 9.1 still apply. As of writing, Verizon certification has been obtained on WP7702. WP7700 Verizon certification is still pending, and the package will be released once the module has been approved by the carrier.

7.1 Software Release Description

7.1.1 Release identification

| Component | Revision |
|------------------------------|--|
| Modem Firmware | SWI9X06Y_02.22.12.00 eaf79c jenkins 2019/04/24 18:48:27 |
| Linux Firmware | SWI9X06Y_02.22.12.00 2019-04-24_20:46:59 |
| MCU Firmware | 002.011 (embedded as a binary in the linux image, not distributed as a separate component) |
| Legato Application Framework | 18.09.2_2a5c6ae47c6da6f1483bc7eac5d48fa1 |
| Binary Size | 50MB (compressed binaries) |
| IMEI SV | 3 |
| Qualcomm Stack Version | MDM9206.LE.2.0-00149-STD.PROD-1.182748.1 |

| | | | |
|-------------|---------|-----------|-------|
| Template #: | 4124005 | Revision: | 01.06 |
|-------------|---------|-----------|-------|



| Component | Revision |
|----------------------|---|
| Linux Kernel Version | Linux swi-mdm9x28-wp 3.18.44 #2 PREEMPT Wed Apr 24 20:48:03 UTC 2019 armv7l GNU/Linux |
| Supported H/W | WP7702, WP7700 |

7.1.2 Software Tools Versions

| S/W Tools Name | Version |
|------------------------|--------------|
| Windows Driver Package | B4836 |
| Windows SDK | None |
| Skylight | None |
| Linux Drivers | S2.35N2.54 |
| Linux SDK | SLQS04.00.17 |

7.1.3 Released Files and Download Processes

| Files | Carrier | Modem Firmware | Config | Linux Distribution | Base Legato System | Comment |
|---|----------------------------|----------------------|-------------|----------------------|--------------------|---------------------------|
| WP7702 Approved | | | | | | |
| WP77xx_Release 11_TMOBILE.exe | GENERIC (T-Mobile) | SWI9X06Y_02.13.02.00 | 001.009_001 | SWI9X06Y_02.22.12.00 | 18.09.2 | T-Mobile USA Approved |
| WP77xx_Release 11_GENERIC_GCF.exe | GENERIC (GCF) | SWI9X06Y_02.22.12.00 | 001.051_000 | SWI9X06Y_02.22.12.00 | 18.09.2 | GCF Approved |
| WP77xx_Release 11_GENERIC_PTCRB.exe | GENERIC (PTCRB) | SWI9X06Y_02.16.06.00 | 001.028_004 | SWI9X06Y_02.22.12.00 | 18.09.2 | PTCRB Approved |
| WP77xx_Release 11_SIERRA.exe | SIERRA | SWI9X06Y_02.22.12.00 | 001.021_000 | SWI9X06Y_02.22.12.00 | 18.09.2 | GCF Approved |
| WP77xx_Release 11_ATT.exe | ATT | SWI9X06Y_02.16.06.00 | 001.026_001 | SWI9X06Y_02.22.12.00 | 18.09.2 | AT&T Approved |
| WP77xx_Release 11_DT.exe | GENERIC (Deutsche Telekom) | SWI9X06Y_02.22.02.00 | 001.041_001 | SWI9X06Y_02.22.12.00 | 18.09.2 | Deutsche Telekom Approved |
| WP77xx_Release 11_VERIZON.exe | VERIZON | SWI9X06Y_02.22.12.00 | 001.042_000 | SWI9X06Y_02.22.12.00 | 18.09.2 | Verizon Approved |
| WP7700 Approved | | | | | | |
| WP77xx_Release 11_GENERIC_GCF.exe | GENERIC (GCF) | SWI9X06Y_02.22.12.00 | 001.051_000 | SWI9X06Y_02.22.12.00 | 18.09.2 | GCF Approved |
| WP77xx_Release 11_GENERIC_PTCRB.exe | GENERIC (PTCRB) | SWI9X06Y_02.16.06.00 | 001.028_004 | SWI9X06Y_02.22.12.00 | 18.09.2 | PTCRB Approved |
| WP77xx_Release 11_SIERRA.exe | SIERRA | SWI9X06Y_02.22.12.00 | 001.021_000 | SWI9X06Y_02.22.12.00 | 18.09.2 | GCF Approved |
| WP77xx_Release 11_ATT.exe | ATT | SWI9X06Y_02.16.06.00 | 001.026_001 | SWI9X06Y_02.22.12.00 | 18.09.2 | AT&T Approved |
| From: https://source.sierrawireless.com/resources/airprime/software/wp77xx/wp77xx-firmware-release-11 | | | | | | |

| | | | |
|-------------|---------|-----------|-------|
| Template #: | 4124005 | Revision: | 01.06 |
|-------------|---------|-----------|-------|



| Function | Files |
|---|--|
| Firmware Components | 9999999_9907618_SWI9X06Y_02.13.02.00_00_GENERIC_001.009_001.spk (T-Mobile USA) 9999999_9907618_SWI9X06Y_02.16.06.00_00_GENERIC_001.028_004.spk (PTCRB) 9999999_9907618_SWI9X06Y_02.22.02.00_00_GENERIC_001.041_001.spk (Deutsche Telekom) 9999999_9907618_SWI9X06Y_02.22.12.00_00_GENERIC_001.051_000.spk (GCF) 9999999_9908788_SWI9X06Y_02.22.12.00_00_SIERRA_001.021_000.spk 9999999_9907787_SWI9X06Y_02.16.06.00_00_ATT_001.026_001.spk 9999999_9908088_SWI9X06Y_02.22.12.00_00_VERIZON_001.042_000.spk linux-SWI9X06Y_02.22.12.00.cwe legato-18.09.2.cwe |
| From: https://source.sierrawireless.com/resources/airprime/software/wp77xx/wp77xx-firmware-release-11 | |

7.1.4 Available Memory

Flash:

| NAME | PARTITION | ALLOCATION (KB) | IMGSIZE (KB) | USAGE |
|------------------|-----------------|-----------------|--------------|-------|
| LK boot | mtd12 (boot) | 14336 | 8957 | 62% |
| Linux Kernel | mtd13 (system) | 29952 | 19456 | 64% |
| Legato Framework | mtd14 (lefwkro) | 8704 | 4609 | 53% |
| SWIRW | mtd15 (swirw) | 24576 | | |
| USERAPP | mtd16 (userapp) | 133120 | | |

RAM:

110912 kB^[1]^[2]

[1] Value is read from the MemAvailable parameter in /proc/meminfo

[2] Values are for reference only and will vary depending on what services/processes are running at the time of measurement

7.2 Software Changes Description

The WP77xx Release 11 is based on modem and Linux versions SWI9X06Y_02.22.10.00. This release is functionally equivalent to WP76xx Release 11, with notable changes and features listed below.

| ID | Title | Description | Impacted Domain |
|--------|-------|-------------|-----------------|
| Legato | | | |

| | | | |
|-------------|---------|-----------|-------|
| Template #: | 4124005 | Revision: | 01.06 |
|-------------|---------|-----------|-------|

| ID | Title | Description | Impacted Domain |
|--|--|---|-----------------|
| Various | Legato 18.09.1 | Legato 18.09.2: <ul style="list-style-type: none"> https://docs.legato.io/18_09/releaseNotes18090.html https://docs.legato.io/18_09/releaseNotes18080.html https://docs.legato.io/18_09/releaseNotes18070.html Upgrade from 18.06.1 in Release 9.1. Includes: <ul style="list-style-type: none"> LE-10931 - Neighbouring cell info API is returning cell info only for serving cell in case of UMTS and LTE mode LE-10514 - Package download is not launched when no application register to AV events. User agreement has been disabled by default in this release LE-12343 - Fix for FOTA download failure in poor network conditions LE-12162 - Suspend package download when curl retry fails | Legato AF |
| ECHO-710 LE-12343 LE-12162 | FOTA Interruption | If FOTA was interrupted for a lengthy duration, such as cases when there was limited network coverage, the download would abort and need to be restarted (rather than resumed). This has been fixed in Legato 18.09.1. | FOTA |
| Linux Distribution | | | |
| QT19X07-2317 QT19X07-2446 QT19X07-2553 | Upgrade Linux Distro to LXSWI2.2-10.0, based on Yocto 2.2.2 | Upgrade to LXSWI2.2-10.0 Includes: <ul style="list-style-type: none"> Enabling QCA9377 WiFi driver Kernel security fixes Smack onlycap capable. | Linux baseline |
| QT19X07-2404 | Incremental build of yocto cannot boot up | When built incrementally, the result yocto.cwe was not bootable due to roothash out of sync. Solution is to add nostamp=1 to force install task of initramfs-mdmunit recipe | Build |
| QT19X07-2197 QT19X07-2273 | Crash when AT port URC on USB during selective suspend | A crash was observed intermittently when using AT over USB and the apps processor came out of sleep to generate a URC (e.g. +CNMI message on incoming SMS). | Kernel |
| QT19X06-164 | Wake-able GPIOs are not working as wakeup interrupt in USB-SS mode | When the device is in USB Selective Suspend mode, the GPIOs that can be configured as wake up interrupts were unable to wake the device from sleep state. This issue has been fixed in this release. GPIO36 and GPIO38 are exceptions and still do not work properly, see QT19X06-167. | GPIO |
| LPM | | | |
| QT19X07-2488 | Set default PSM synchronization option to use MCU RTC Alarm as the PSM wakeup source | Change the default PSM/ULPM synchronization option in the driver to use the MCU RTC Alarm as the PSM wakeup source for minimal current consumption during PSM. | PSM/ULPM |

| ID | Title | Description | Impacted Domain |
|---|--|---|-------------------|
| QT19X07-2551 | PSM does not work | <p>In Sierra-customized PSM power off sequence, "poweroff" command is used for graceful Linux system shutdown after MPSS shuts down. The script for "poweroff" command will synchronize with MPSS to start power-down. In case of the customized PSM power off sequence, MPSS may have shut down at the point of "poweroff" command is issued, causing a fatal error detected by BAM DMUX kernel driver and then recovered with a system-restart.</p> <p>This patch adds a Boolean flag to prevent the BAM DMUX kernel driver from restarting system, knowing that MPSS may have been shut down at this point. The added flag is set only during the customized PSM power off sequence. It has no impact on regular "poweroff" command.</p> | PSM/ULPM |
| QT19X06-141 | AT!POWERMODE and boot_source/enable doesn't take effect for PSM or ULPM fallback | This fixes the issue where PSM cannot be enabled or disabled by Legato or AT!POWERMODE | PSM/ULPM |
| QT19X06-152 | ULPM fallback does not work consistently | When PSM with ULPM fallback is attempted, if PSM is not available, ULPM shall be used to enter ULPS. However this fallback to ULPM was not working consistently. This has been fixed in Release 11. | PSM/ULPM |
| Modem | | | |
| Core | | | |
| QT19X06-12 QT19X06-29 QT19X06-68 QT19X06-116 | Multiple Qualcomm updates to: MDM9206.LE.2.0-00149-STD.PROD-1.182748.1 | Add Qualcomm baseline MDM9206.LE.2.0-00149-STD.PROD-1.182748.1. Includes: <ul style="list-style-type: none"> ECHO-702: Verizon Signalling Test case 2.11 failure CERTREQ-819: [AT&T] - Qualcomm CR Update: July 2018 QT19X06-3: Anatel IPV6 CRs ECHO-700: Fix for modem crash assertion fails in dlch.c due to pdsch_semaphore_value | Qualcomm baseline |
| Protocol/Certification | | | |
| QT19X06-3 | Corner case failures in RFC2460 IPV6 compliance tests | WP77 was not compliant with some corner case requirements in RFC2460 for IPV6 protocol testing. These issues have been fixed in this release, with the exception of test case v6LC_1_2_01 in GSM. | Data |
| QT19X06-18 | Increase IMEI SV to 3 | The IMEI SV has been increased to 3 in this release. | IMEI SV |
| QT19X07-2364 | Update TS.25 list to October 01, 2018 | Default TS.25 list updated. Non-GSMA PLMNs removed except Test PLMNs. | GCF |

| ID | Title | Description | Impacted Domain |
|--|--|--|-----------------|
| Various | Verizon Carrier LWM2M Support | <p>The full support for Carrier LWM2M has been added in this Release. The Carrier LWM2M client is only enabled for the Verizon carrier image and is a mandatory requirement to obtain Verizon certification. It is disabled by default for all other carriers.</p> <p>Notable features include:</p> <ul style="list-style-type: none"> • Runtime credential provisioning from SIM • SMS wakeup • Registration update and recovery • Server object 1 • Device Management object 3 • Connectivity Monitoring object 4 • Connectivity Statistics object 7 • Observation and Notification <p>Although WP77xx Release 11 is feature complete for Carrier LWM2M, WP76xx Release 11 only contains partial functionality and does not meet Verizon's OTADM requirements.</p> | Carrier LWM2M |
| UIM | | | |
| QT19X07-698 QT19X07-2041 QT19X07-2112 | Auto SIM switching, v. 1 | <p>A feature has been added in advance of embedded SIM module deployments that allows configuration of a preferred SIM such that upon boot, if both external SIM and embedded SIM are present, the preferred one will be selected. See AT!CUSTOM="UIMAUTOSWITCH" in the WP AT Command Guide.</p> <p>Changes in SIM detect status at run time do not trigger SIM reselection. This is being considered in a future release.</p> | eSIM |
| QT19X07-1705 QT19X07-2215 QT19X07-2241 | Unable to support SIM hot swap on external SIM2 slot | Fixed the issue that SIM in external multiplexed slot 2 does not work when removing SIM in primary slot 1 | SIM |
| QT19X06-120 | Crash in dog.c: Watchdog detects task starvation of 839ce864 | Early access of some slow SIM cards that takes more than 10s to initialize will cause a crash due to watchdog timeout. The blocking calls have been removed in the code to prevent this. | Stability |
| IO | | | |
| QT19X07-2030 | External GPIO config is not persistent for image switches | In previous releases, any firmware update or image switch would clear all configuration in AT+WIOCFG. Now, when upgrading to Release 11 and future releases, this configuration will persist. That is, modules running Release 9 or earlier will retain their configuration when upgrading to Release 11. | GPIO |
| QT19X07-1410 QT19X07-2124 QT19X07-2131 | Embedded linux assigned GPIO initialization on boot | <p>In Release 7, issues with embedded linux assigned GPIOs (e.g. QT19X07-959, QT19X07-1121) were addressed by re-initializing them late in modem startup. This, however, introduced a potential timing issue with linux if an attempt to set them early in linux boot occurred before the final modem initialization.</p> <p>These are now initialized in the boot loader to ensure no such timing conflict occurs.</p> | GPIO, Linux |

| ID | Title | Description | Impacted Domain |
|------------------------------|---|--|----------------------|
| QT19X07-1770 | Add GPIO4 support | For WP75/85 GPIO4 (CF3 pin 65) is hardcoded for use as UIM2 detect line. For WP76/77, however, UIM2 is reserved for embedded SIM and therefore not needed for this purpose. It has therefore been exposed as a GPIO. This is supported via AT+WIOCFG and sys/class/gpio as with other GPIOs, but will only be available on new units shipped with Release 11 or later. Future use for SIM2 detection in conjunction with AT+KSIMSEL is under consideration (QT19X07-1705). | GPIO |
| QT19X06-22 | Issues with Band Selection output pins on GSM | In previous firmware releases, the mapping of the GSM active band to the 3GPP band number is incorrect, so the wrong bands might be shown as active. Also, the pins are not activated during TX period on GSM bands. This has been fixed. | GPIO |
| Security | | | |
| QT19X07-1997 | Security: move DM disable to Level 2 via AT!USBCOMP | As the DM port poses a security risk, the ability to configure it is lock level 3. However, if it happens to be enabled, it is important for security purposes to be able to close it, so disable is moved to lock level 2. | Boot |
| QT19X07-1875 | No limit to secure storage | Previously there was no limit imposed on SFS so once consumed would impact internal features unexpectedly, such as AGPS. This change imposes a 512KB limit on customer SFS content. The limit is not configurable. If that limit has already been exceeded prior this firmware update it must be reduced prior to updating SFS. | SFS |
| QT19X07-2160 | Reduce AT!SECBOOTCFG? to a level 2 lock | Secure boot devices have limited debug capability unless loaded with a debug image built specifically for that module. Such debug images can only be built by Sierra and may require information provided by AT!SECBOOTCFG? so this query command has been reduced to lock level 2 for field support. | Secure boot |
| QT19X07-3238 OEMPRI-11148 | [Secure Boot] Increase safe update signature buffer | In previous WP77xx releases, enabling Customer Secure Boot (OEM Authentication) will cause the device to unable to boot up due to an issue in processing the keystore file. Customers who wish to enable Customer Secure Boot must upgrade their firmware to Release 11 or later prior to downloading the keystore file. All the carrier packages in Release 11 have been repackaged with the new bootloader to fix this issue. | Customer Secure boot |
| Data | | | |
| OEMPRI-8614 OEMPRI-8464 | APN in CGDCONT changed after a FOTA | Due to the current design, a manually updated APN profile in the Generic PRI with embedded Sierra PRI would be reverted to the Sierra default if a Sierra SIM was detected. To ensure APN persistence across FW updates / image switches a separate SIERRA carrier PRI was created. Both Generic and Sierra images must be loaded to have separate APN profiles for both. | Carrier PRI |

| | | | |
|-------------|---------|-----------|-------|
| Template #: | 4124005 | Revision: | 01.06 |
|-------------|---------|-----------|-------|

| ID | Title | Description | Impacted Domain |
|--|--|--|-----------------|
| OEMPRI-9073 OEMPRI-9225 OEMPRI-11103 | Update Generic and Sierra PRI so SELRAT and SELCIOT is persistent | Due to the initial long network scan time on LTE NB1, some users choose to disable NB1 mode for a quicker acquisition time. This setting was reset after a FW upgrade, so the device would fail to re-attach to the network immediately after a FOTA download. Change was made to make the LTE mode selection and RAT preference persistent so NB1 scanning won't be triggered again after the FOTA. | Carrier PRI |
| OEMPRI-11071 | Update Sierra APN to lp.swir | Default APN for users using the Sierra PRI has been changed to "lp.swir". | Carrier PRI |
| QT19X06-20 | SLQSAutoConnect() or SetAutoconnect() always returns error code 1071 | Support for the SLQS auto-connect related APIs were previously disabled on the chipset by Qualcomm. This has since been enabled. | QMI |
| AT Commands | | | |
| QT19X06-69 | LTE ACQ DB EFS file format is handled incorrectly in ACQCHAN command | The AT!ACQCHAN command output was previously unable to show the LTE channels due to a file parsing error. This has been fixed. | AT |
| Factory/Configuration | | | |
| QT19X06-72 | NVTHIST does not survive a firmware update | The file to record device configuration history was previously only backed up at the Sierra factory. This has since been changed so that customers can make persistent changes to this file to track their own additional configuration history to the device. | NV |

7.3 Security Corrections/Improvements

| CVE | Description |
|--------------------------------|---|
| CVE-2018-5916 | Information Exposure in MODEM |
| CVE-2018-11268 | Improper Validation of Array Index in Storage |
| CVE-2018-11267 | Improper Validation of Array Index in Core |
| CVE-2018-5866 | Untrusted Pointer Dereference in TrustZone |
| CVE-2018-5914 | Improper Validation of Array Index in TZ CORE |
| CVE-2018-5915 | Reachable Assertion in MODEM IP Stack |
| CVE-2018-11966 | Improper Input Validation in MMCP |
| CVE-2018-11945 | Buffer Copy Without Checking Size of Input in MMCP |
| CVE-2018-11938 | Buffer Copy Without Checking Size of Input in Trusted Application Environment |
| CVE-2018-11289 | Buffer Copy Without Checking Size of Input in Core |
| CVE-2018-5913 | Cryptographic Issues in TrustZone |
| CVE-2018-11820 | Cryptographic Issues in Ecosystem |
| CVE-2018-13886 | Integer Overflow to Buffer Overflow in MODEM |
| CVE-2018-13887 | Integer Overflow or Wraparound in MODEM |
| CVE-2018-13903 | Null Pointer Dereference in Modem |
| CVE-2018-13923 | Use of Initialized Data in MODEM |

| CVE | Description |
|----------------------------------|--|
| CVE-2018-11968 | Integer Overflow or Wraparound in WLAN |
| CVE-2018-5897 | Buffer over-read while reading data from buffer in dci_process_ctrl_status() |
| CVE-2018-5896 | Possibility of out-of-bound read because of not validating source buffer length |
| CVE-2018-5864 | Improper Restriction of Operations within the Bounds of a Memory Buffer in WLAN |
| CVE-2018-11266 | Improper Input Validation in DIAG |
| CVE-2018-11265 | Buffer Copy Without Checking Size of Input in Core |
| CVE-2018-5919 | Use After Free in WLAN |
| CVE-2018-11953 | Buffer Over-read in WLAN |
| CVE-2018-11885 | Reachable Assertion in WLAN |
| CVE-2017-1000158 | CPython (aka Python) up to 2.7.13 is vulnerable to an integer overflow in the PyString_DecodeEscape function in stringobject.c, resulting in heap-based buffer overflow |
| CVE-2018-1000030 | Python 2.7.14 is vulnerable to a Heap-Buffer-Overflow as well as a Heap-Use-After-Free. |
| CVE-2016-10255 | The __libelf_set_rawdata_wlock function in elf_getdata.c in elfutils before 0.168 allows remote attackers to cause a denial of service (crash) via a crafted (1) sh_off or (2) sh_size ELF header value, which triggers a memory allocation failure. |
| CVE-2016-10254 | The allocate_elf function in common.h in elfutils before 0.168 allows remote attackers to cause a denial of service (crash) via a crafted ELF file, which triggers a memory allocation failure. |
| CVE-2018-1000120 | A buffer overflow exists in curl 7.12.3 to and including curl 7.58.0 in the FTP URL handling that allows an attacker to cause a denial of service or worse. |
| CVE-2018-1000122 | A buffer over-read exists in curl 7.20.0 to and including curl 7.58.0 in the RTSP+RTP handling code that allows an attacker to cause a denial of service or information leakage |
| CVE-2018-1000121 | A NULL pointer dereference exists in curl 7.21.0 to and including curl 7.58.0 in the LDAP code that allows an attacker to cause a denial of service |
| CVE-2017-5601 | An error in the lha_read_file_header_1() function (archive_read_support_format_lha.c) in libarchive 3.2.2 allows remote attackers to trigger an out-of-bounds read memory access and subsequently cause a crash via a specially crafted archive. |
| CVE-2016-10350 | The archive_read_format_cab_read_header function in archive_read_support_format_cab.c in libarchive 3.2.2 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted file. |
| CVE-2016-10349 | The archive_le32dec function in archive_endian.h in libarchive 3.2.2 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted file. |
| CVE-2018-6485 | An integer overflow in the implementation of the posix_memalign in memalign functions in the GNU C Library (aka glibc or libc6) 2.26 and earlier could cause these functions to return a pointer to a heap area that is too small, potentially leading to heap corruption. |
| CVE-2017-15804 | The glob function in glob.c in the GNU C Library (aka glibc or libc6) before 2.27 contains a buffer overflow during unescaping of user names with the ~ operator. |
| CVE-2018-1000001 | In glibc 2.26 and earlier there is confusion in the usage of getcwd() by realpath() which can be used to write before the destination buffer leading to a buffer underflow and potential code execution. |
| CVE-2017-12133 | Use-after-free vulnerability in the clntudp_call function in sunrpc/clnt_udp.c in the GNU C Library (aka glibc or libc6) before 2.26 allows remote attackers to have unspecified impact via vectors related to error path. |
| CVE-2017-15107 | A vulnerability was found in the implementation of DNSSEC in Dnsmasq up to and including 2.78. Wildcard synthesized NSEC records could be improperly interpreted to prove the non-existence of hostnames that actually exist. |

| CVE | Description |
|--------------------------------|---|
| CVE-2018-7738 | In util-linux before 2.32-rc1, bash-completion/umount allows local users to gain privileges by embedding shell commands in a mountpoint name, which is mishandled during a umount command (within Bash) by a different user, as demonstrated by logging in as root and entering umount followed by a tab character for autocompletion. |
| CVE-2017-12424 | In shadow before 4.5, the newusers tool could be made to manipulate internal data structures in ways unintended by the authors. Malformed input may lead to crashes (with a buffer overflow or other memory corruption) or other unspecified behaviors. This crosses a privilege boundary in, for example, certain web-hosting environments in which a Control Panel allows an unprivileged user account to create subaccounts. |
| CVE-2018-0739 | Constructed ASN.1 types with a recursive definition (such as can be found in PKCS7) could eventually exceed the stack given malicious input with excessive recursion. This could result in a Denial Of Service attack. There are no such structures used within SSL/TLS that come from untrusted sources so this is considered safe. Fixed in OpenSSL 1.1.0h (Affected 1.1.0-1.1.0g). Fixed in OpenSSL 1.0.2o (Affected 1.0.2b-1.0.2n). |
| CVE-2017-16544 | In the add_match function in libbb/lineedit.c in BusyBox through 1.27.2, the tab autocomplete feature of the shell, used to get a list of filenames in a directory, does not sanitize filenames and results in executing any escape sequence in the terminal. This could potentially result in code execution, arbitrary file writes, or other attacks. |

7.4 Known Issues

This section presents all known issues in this release.

| ID | Title | Description | Impacted Domain |
|----------------------|---|--|-----------------|
| Bugs | | | |
| ECHO-712 LE-11902 | AVMS Heartbeat doesn't work for periods >= 4 hr | <p>On some networks including the Sierra Wireless Core network, the network will detach the device after a period of inactivity. Legato currently cannot handle such a scenario and therefore polling will commonly fail on those networks if it is set to longer than 4 hours.</p> <p>This issue does not affect customers who are using PSM on their devices.</p> <p>Customers who do not use PSM and are not power sensitive are advised to configure their polling timer to a period shorter than 4 hours.</p> <p>This issue will be fixed in the Legato 19.02 release. For the Sierra Wireless core network, this is expected to be resolved in the future where the timeout will be extended significantly on LPWA APNs.</p> | FOTA |
| ECHO-708 LE-12462 | [VERIZON] Synchronization failed on attempt to retrieve data object of IMSI (Iwm2m.10241.0.2) | Legato is unable to read the IMSI from some SIM cards that contain a CSIM application which is listed first, such as some of Verizon's SIM cards. This in turn will cause synchronization failures with the Airvantage server. Expectation is this will be resolved in a future Legato release. | Connectivity |

| ID | Title | Description | Impacted Domain |
|----------------------|--|---|-----------------|
| ECHO-757 ECHO-770 | Unable to resume a FOTA download after failure in the middle of a previous download process | The Legato 18.09 release does not support resuming a FOTA job if it fails in the middle of a package download. If a FOTA download fails due to events including, but not limited to, device reset, power loss, or AirVantage connection problems, the download will appear to resume but will end up failing. When this happens, the FOTA job must be restarted (rather than resumed). This has been fixed in the Legato 19.02 release. | FOTA |
| QT19X06-33 | Connectivity Interruption | In lab testing, a scenario has been occasionally observed where connectivity is interrupted every three minutes when using the Sierra Wireless SIM. This issue has not been seen in field testing. A corrective plan is currently ongoing, get in touch with your Sierra Wireless representative for latest update | Connectivity |
| QT19X07-2696 | Modem Daemon crashes when le_mdc_GetDisconnectionReason function has been called | Modem daemon in Linux will crash when querying the disconnection reason from Legato. The recovery after the crash is automatic and there should be no impact to customers. | Legato |
| QT19X07-2535 | Unable to build Yocto image with QCA9377_BUILD enabled | Unable to build with QCA9377 wifi driver enabled. | Yocto |
| QT19X07-2387 | After starting the data session - AUTHENTICATION <LE_MDC_AUTH_CHAP LE_MDC_AUTH_PAP> ENABLED, the profile returned is incorrect | With Legato, fail to establish a data session with authentication enabled | Legato |
| ECHO-672 | RFC 2460 Compliance test case v6LC_1_2_01 failure | The device is currently failing test case v6LC_1_2_01 for IPV6 RFC 2460 compliance due to failure to send a Parameter Problem message during the test. | Data |
| QT19X06-167 | Interrupts for wake-able GPIOs 36 and 38 must be re-enabled | For wake-able GPIOs 36 and 38, the interrupt can be only be detected once after a USB suspend/resume cycle. Workaround is to explicitly re-enable the interrupt (as done in the gpioCf3SSDemo sample app). This issue exists in Release 9.1 as well. | GPIO |
| QT19X07-2327 | Can't attach Bluetooth controller to UART2 | User currently cannot attach the Bluetooth controller to UART2, but it works on UART1. Issue is due to lack of high speed UART configuration setting in the device tree for UART2, that currently only uses low speed 2-wire configuration. | UART/Console |
| QT19X07-2303 | Cannot input characters to UART2 while the module is in sleep mode | UART2 mapped as linux console cannot input character when the module is in sleep. | UART/Console |
| QT19X07-2272 | Periodic high current draw when testing EDRX/DRX with HSIC Enabled | Periodic high current draw is seen when testing EDRX/DRX with HSIC Enabled. Every 3.5 mins, there will be a period of 1.5 mins where the device will wake up and consume around 35mA of current. | System |

| | | | |
|-------------|---------|-----------|-------|
| Template #: | 4124005 | Revision: | 01.06 |
|-------------|---------|-----------|-------|

| ID | Title | Description | Impacted Domain |
|--------------|---|--|-----------------|
| QT19X07-2245 | Missing libxml during incremental build | Incremental build will fail when building Yocto, the customer will need to clean & rebuild for every Yocto change. A temporary workaround is to backup and restore libxml.la for avoiding a clean build. | Build |
| QT19X07-2195 | SNTP Client unable to use existing connection | Unlike the WPx5, the WP76/77 SNTP client must open a new connection, which is more visible and could have undesirable consequences. Therefore for WP76 the feature is off by default so the user would need to enable it explicitly to get the benefit. This can be done via QMI/Legato, but because it is a AT!CUSTOM feature, a level 2 password is required to enable it via AT | FOTA/Other |
| QT19X07-2186 | Setting identical profile AUTH params forces LTE re-attach with SINGLEAPNSWITCH | With SINGLEAPNSWITCH feature enabled, Legato cm data connect always fails on LTE with Legato 18.05.1 or older | Legato |
| QT19X07-2076 | No Legato Event after an OPEN CHANNEL | No Legato event is reported for STK BIP Open Channel proactive command | Legato |
| QT19X07-1928 | The eth0 address is erased when Wifi chip is inserted after reboot | eth0 address is erased when Wifi chip is inserted after reboot | Driver |
| QT19X07-1494 | Legato - boot loop error when build with 70MB Database | Boot loop error when build Legato image with 70MB Database | Legato |
| QT19X07-2474 | Current can only reach around 15 mA when it supposes to go to sleep | Modules fail to enter sleep mode after SIM card being unlocked and then synchronizing to the network. | Sleep |
| QT19X07-3315 | AT!CUSTOM BANDSELEN not persistent over FW upgrades | The setting of AT!CUSTOM="BANDSELEN",1 to enable Antenna Select feature will not stay persistent across a firmware upgrade. Customers who are using this customization will need to either manually enable it again, or request to have persistence added for this setting in their OEM PRI to avoid this issue. | NV |

8 SWI9X06Y Release 9.1

Release 9.1 is a point release based off Release 9 that is certified for PTCRB and GCF on WP7700 and WP7702. This is also the AT&T final carrier approval candidate. The Linux and Legato images packaged in this release is the same as WP76xx and WP77xx Release 10.



8.1 Software Release Description

8.1.1 Release identification

| Component | Revision |
|------------------------------|--|
| Modem Firmware | SWI9X06Y_02.16.06.00 7605a6 jenkins 2018/06/20 17:56:12 |
| Linux Firmware | SWI9X06Y_02.18.05.00 2018-07-20_21:00:21 |
| MCU Firmware | 002.009 (embedded as a binary in the linux image, not distributed as a separate component) |
| Legato Application Framework | 18.06.1_7bc924287cc41a0157bd414af840e754 |
| Binary Size | 50MB (compressed binaries) |
| IMEI SV | 2 |
| Qualcomm Stack Version | MDM9206.LE.2.0-00122-STD.PROD-1.153866.1.155657 |
| Linux Kernel Version | Linux swi-mdm9x28-wp 3.18.44 #2 PREEMPT Fri Jul 20 21:01:16 UTC 2018 armv7l GNU/Linux |
| Supported H/W | WP7702, WP7700 |

8.1.2 Software Tools Versions

| S/W Tools Name | Version |
|------------------------|--------------|
| Windows Driver Package | B4836 |
| Windows SDK | None |
| Skylight | None |
| Linux Drivers | S2.33N2.52 |
| Linux SDK | SLQS04.00.15 |

8.1.3 Released Files and Download Processes

| Files | Carrier | Modem Firmware | Config | Linux Distribution | Base Legato System | Comment |
|---|----------------------|----------------------|-------------|----------------------|--------------------|-------------------------|
| WP7702 Approved/Pending | | | | | | |
| WP77xx_Release 9.1_TMOBILE.exe | GENERIC (T-Mobile) | SWI9X06Y_02.13.02.00 | 001.009_000 | SWI9X06Y_02.18.05.00 | 18.06.1 | T-Mobile Approved |
| WP77xx_Release 9.1_PTCRB_GCF.exe | GENERIC (PTCRB, GCF) | SWI9X06Y_02.16.06.00 | 001.028_001 | SWI9X06Y_02.18.05.00 | 18.06.1 | GCF and PTCRB Approved |
| WP77xx_Release 9.1_ATT_test.exe | ATT | SWI9X06Y_02.16.06.00 | 001.026_000 | SWI9X06Y_02.18.05.00 | 18.06.1 | AT&T Approval - Pending |
| WP7700 Approved/Pending | | | | | | |
| WP77xx_Release 9.1_PTCRB_GCF.exe | GENERIC (PTCRB, GCF) | SWI9X06Y_02.16.06.00 | 001.028_001 | SWI9X06Y_02.18.05.00 | 18.06.1 | GCF and PTCRB Approved |
| WP77xx_Release 9.1_ATT_test.exe | ATT | SWI9X06Y_02.16.06.00 | 001.026_000 | SWI9X06Y_02.18.05.00 | 18.06.1 | AT&T Approval - Pending |
| From: https://source.sierrawireless.com/resources/airprime/software/wp77xx/wp77xx-firmware-release-9.1 | | | | | | |

| | | | |
|-------------|---------|-----------|-------|
| Template #: | 4124005 | Revision: | 01.06 |
|-------------|---------|-----------|-------|



| Function | Files |
|---|---|
| Firmware Components | 9999999_9907618_SWI9X06Y_02.13.02.00_00_GENERIC_001.009_000.spk (T-Mobile) 9999999_9907618_SWI9X06Y_02.16.06.00_00_GENERIC_001.028_001.spk (PTCRB, GCF) 9999999_9907787_SWI9X06Y_02.16.06.00_00_ATT_001.026_000.spk linux-SWI9X06Y_02.18.05.00.cwe legato-18.06.1.cwe |
| From: https://source.sierrawireless.com/resources/airprime/software/wp77xx/wp77xx-firmware-release-9.1 | |

8.2 Software Changes Description

The WP77xx Release 9.1 is based on modem version SWI9X06Y_02.16.06.00 and Linux version SWI9X06Y_02.18.05.00. Notable changes and features are listed below.

| ID | Title | Description | Impacted Domain |
|--|--|--|---------------------|
| Legato | | | |
| Various | Legato 18.06.1 | Legato 18.06.1 <ul style="list-style-type: none"> https://docs.legato.io/latest/releaseNotes18061.html https://docs.legato.io/latest/releaseNotes18051.html https://docs.legato.io/latest/releaseNotes18040.html Upgrade from 18.03.0 in Release 9. Includes: <ul style="list-style-type: none"> LE-10549/LE-10671: Secure storage corrupted after package update LE-10462: QMI indication for AVMS binary update session does not set correct binary type | Legato AF |
| Linux Distribution | | | |
| QT19X07-1885 QT19X07-2036 | Move MCU firmware default location | Previously, the MCU image was stored in the USERRW partition. It has now been moved to ROOTFS. This provides the benefit of freeing USERRW for the end user and ensuring that the correct MCU image is paired with the corresponding linux kernel driver instead of being distributed/packaged independently. | MCU file management |
| QT19X07-2089 QT19X07-2104 QT19X07-2142 | Unable to build from tarball | The externally posted linux source distribution (tarball) failed to build. This has been corrected. | Build |
| QT19X07-2002 | Legato Toolchain Versioning | Instead of always using the default location /opt/swi/y22-ext, the toolchain is now installed in a version specific location, e.g. /opt/swi/SWI9X06Y_02.18.05.00 | Build |
| QT19X07-2053 QT19X07-2177 | Upgrade Linux Distro to LXSWI2.2-7.0, based on Yocto 2.2.2 | Upgrade to LXSWI2.2-7.0 (from LXSWI2.2-4.0 in Release 9) | Linux Baseline |
| QT19X07-2197 QT19X07-2273 | Crash when AT port URC on USB during selective suspend | A crash was observed intermittently when using AT over USB and the apps processor came out of sleep to generate a URC (e.g. +CNMI message on incoming SMS). | Kernel |

| | | | |
|-------------|---------|-----------|-------|
| Template #: | 4124005 | Revision: | 01.06 |
|-------------|---------|-----------|-------|

| ID | Title | Description | Impacted Domain |
|--|---|--|-------------------|
| QT19X07-2217 | Module cannot resume sleep after ending a voice call if no codec on host platform | In the case where no codec is installed on the host platform, after a voice call has ended the module could not go back to sleep mode. This has been fixed in the linux kernel alsa driver. | Kernel |
| QT19X07-1862 | Boot up time optimization: load modem image after partition mounted | By starting modem loading earlier, as soon as the image partition is mounted, the system boot time can be reduced by ~1.5 seconds | Boot |
| Modem | | | |
| Core | | | |
| QT19X07-2163 | Add Qualcomm MDM9206.LE.2.0-00122.1.153866.1.155657 | Add Qualcomm baseline MDM9206.LE.2.0-00122.1.153866.1.155657. Includes: <ul style="list-style-type: none"> • QT19X07-1818: [36.523-1][22.3.2.2][NB-IOT] AM RLC TC failure • QT19X07-1821: [36.523-1][22.4.8][NB-IOT] RRC conn establishment/Access barring • QT19X07-1498: [36.523-1][7.1.2.4] Step2 SS Unexpected Receive L1 indication at port SYSIND | Qualcomm baseline |
| IO | | | |
| QT19X07-2030 | External GPIO config is not persistent for image switches | In previous releases, any firmware update or image switch would clear all configuration in AT+WIOCFG. Now, when upgrading to Release 9.1 and future releases, this configuration will persist. That is, modules running Release 9 or earlier will retain their configuration when upgrading to Release 9.1. | GPIO |
| QT19X07-1410 QT19X07-2124 QT19X07-2131 | Embedded linux assigned GPIO initialization on boot | In Release 7, issues with embedded linux assigned GPIOs (e.g. QT19X07-959, QT19X07-1121) were addressed by reinitializing them late in modem startup. This, however, introduced a potential timing issue with linux if an attempt to set them early in linux boot occurred before the final modem initialization. These are now initialized in the boot loader to ensure no such timing conflict occurs. | GPIO, Linux |
| UART | | | |
| QT19X07-2136 | Modem reset when using UART1 | A bug in the CTS interrupt handler was causing a reset when using UART1 in some cases. This has been fixed in the kernel. | UART |
| Temperature | | | |
| QT19X07-2054 | Modules in airplane mode crash at high temperature | At high ambient temperatures (> 70C) in airplane mode (not necessarily due to thermal mitigation) some modules would reset due to DDR instability at low frequency (<48MHz). A fix was added to block low DDR frequency selection at high temperatures. | High Temp |
| Low Power Modes | | | |

| ID | Title | Description | Impacted Domain |
|------------------------------|---|---|-----------------|
| QT19X07-1709 | persist ULPS wakeup triggers | In the original ULPS implementation where wake up triggers would be set before every ULPS request there was no need to persist this configuration. With the harmonization with PSM, however, re-entry to the ultra low power state is automatic (with any explicit command from the user) and hence persistence of wakeup triggers across cycles is necessary. They will now continue to remain in effect until explicitly cleared. | PSM/ULPS |
| QT19X07-2017 | Add command to clear all ULPS wake up sources | Wake up sources are persisted across PSM/ULPS cycles unless explicitly cleared. To simplify this operation support has been added to clear all sources in a single command via AT command or sysfs: a) AT!POWERWAKE=0 b) echo 7 > /sys/module/swimcu_pm/boot_source/clear Note that while documentation of previous releases stated that AT!POWERWAKE=0 would clear all sources, it in fact only cleared the ADC. This has now been fixed. | PSM/ULPS |
| QT19X07-1678 QT19X07-2035 | PSM status code | The addition of PSM support introduces additional complexity with network interaction. To get better insight into the current status, and in particular reasons why a PSM request was rejected, a status code is made available via sysfs: /sys/module/swimcu/psm/status | PSM |
| QT19X07-1955 | Add extended PSM configuration support | Some extended PSM features were previously not configurable or persistent. The only such feature currently used in WP77 is early wake up time. With this change, the early wakeup time is now increased to ensure the TAU timer is not missed. | PSM |

8.3 Known Issues

This section presents all known issues in this release.

| ID | Title | Description | Impacted Domain |
|------------------------------|--------------------------------|--|------------------|
| Bugs | | | |
| QT19X07-1653 QT19X07-2156 | Instability at low temperature | Intermittent instability issues have been observed at low temperature (below -20C), including loss of sync in sleep mode, and UART not working on boot. Test results to date have been inconclusive. Investigation is ongoing. | Connectivity |
| QT19X07-2159 | Anatel IPv6 failure | WP is not in compliance with latest Anatel (Brazil regulatory) IPv6 requirements | Wireless Network |

| ID | Title | Description | Impacted Domain |
|--|--|--|-----------------|
| QT19X07-1764 | New MAC Address generated on each power cycle | By default, the WP will generate a new MAC address on the ethernet interface on every boot. This may be fixed by preconfiguring a MAC address in /etc/network/interfaces | Wired Network |
| QT19X07-2300 | UART1 cannot suspend after RX wakeup | Normally while idle, the UART will suspend to save power, however currently, after first waking up on RX data, it will no longer automatically suspend, incurring an extra ~12mA. | UART |
| QT19X07-2185 QT19X07-2223 QT19X07-2242 | PSM lowest power mode Issues | The PSM lowest power mode option was added in Release 9 to achieve ~7uA. Subsequent testing has found this mode has issues with missing TAU complete message and time of day continuity across PSM cycles. While these issues will continue to be worked for a future release (linux update) the previous default option (consuming ~16uA) has been restored. | PSM |
| LXSWIREF-684 | Patching kernel using recipe linux-quick does not work anymore | Patching the Yocto kernel by using a .bbappend with SRC_URI in recipe linux-quick does not work. The linux image builds, but will not boot on the target. This was introduced in Release 9. A workaround is available upon request from Sierra support. It will be fixed in the next release. | Build |
| QT19X07-1308 | Missing Java dependency for building LK bootloader | The Android Signing tools for the LK bootloader require Java Runtime Environment (JRE) to be installed on the host platform. JRE has not been added to the build environment, so must be installed on the build machine manually. Example, for Ubuntu 16.04: sudo apt-get install default-jre <i>Manual JRE installation will continue to be required going forward.</i> | Build |
| QT19X07-2102 | Workaround issues in GPIO control from linux | Different versions of a workaround were provided to allow linux control of GPIOs with carrier certified modem images. With the issue now addressed in the new carrier certified modem version the workaround is not required, however for workarounds using AT+WIOCFG=<gpio>,0 to enable linux access, these will need to be changed back to AT+WIOCFG=<gpio>,16 going forward. The setting will subsequently be persistent across upgrades so this would be a one time action when upgrading to Release 9.1 | GPIO |



| ID | Title | Description | Impacted Domain |
|--------------|---|---|-----------------|
| QT19X07-1007 | PCM configuration not allowed by default | The ability to set a profile to use a particular interface is controlled by AT!AVPIFACEPREF (level 2 access). By default, PCM was not included so PCM could not be set with AT!AVCFG without first setting AT!AVPIFACEPREF=F. The factory default has been updated to make PCM available by default, however this will only benefit newly manufactured units so AT!AVPIFACEPREF=F is still required. | Audio |
| QT19X07-1494 | Legato - boot loop error when built with large database | Customer legato.cwe image must be small enough to fit into the LEFWKRO partition (8MB). | Legato |
| QT19X07-1278 | Accessing MCU causes I2C NACK error | Any time the MCU is accessed (for version info, GPIO read/write, etc) from a MCU low power state, the first access is needed to wake it up. The retry is automatic and succeeds, but a kernel error is generated on the first attempt. This can be annoying as it floods the kernel log. | Kernel |
| ECHO-621 | WP7702 crashes after issuing AT!DASBAND | During FTM testing, the device will crash when selecting the band under test using AT!DASBAND. Investigation is ongoing with Qualcomm. As a workaround, allow the device to crash once (resets once). Upon the reset, the AT!DASBAND command will not crash the second time around. | FTM |
| ECHO-594 | spidev1.0 does not show up on WP77XX | The spidev kernel module is not loaded on wp77xx Legato targets. As a result, users will not be able to use the SPI service to read and write from the SPI bus. This will be fixed in Legato 18.08. | SPI |

9 SWI9X06Y Release 9

Release 9 includes a number of new features including PDN data multiplexing, QMI support for some existing features, PSM current consumption enhancements as well as several bug fixes. This release is intended as a PTCRB and AT&T final certification candidate to resolve several issues for carrier and industrial certification testing. It is important to note that:

- No GCF and PTCRB certification has been granted yet.
- AirVantage and FOTA is now supported

9.1 Software Release Description

9.1.1 Release identification

| Component | Revision |
|----------------|---|
| Modem Firmware | SWI9X06Y_02.16.04.00 019853 jenkins 2018/05/15 19:28:37 |
| Linux Firmware | SWI9X06Y_02.16.02.00 2018-05-02_12:35:16 |

| | | | |
|-------------|---------|-----------|-------|
| Template #: | 4124005 | Revision: | 01.06 |
|-------------|---------|-----------|-------|



| Component | Revision |
|------------------------------|---|
| MCU Firmware | 002.009 |
| Legato Application Framework | 18.03.0_8c7b8ac619d8a7402ad0dc6f42ba6daf |
| Binary Size | 50MB (compressed binaries) |
| IMEI SV | 2 |
| Qualcomm Stack Version | MDM9206.LE.2.0-00122-STD.PROD-1.149002.1 |
| Linux Kernel Version | Linux swi-mdm9x28 3.18.44 #2 PREEMPT Wed May 2 12:36:47 UTC 2018 armv7l GNU/Linux |
| Supported H/W | WP7702 DV1.1+ WP7700 DV 2.1+ |

9.1.2 Software Tools Versions

| S/W Tools Name | Version |
|------------------------|--------------|
| Windows Driver Package | B4773 |
| Windows SDK | None |
| Skylight | None |
| Linux Drivers | S2.31N2.50 |
| Linux SDK | SLQS04.00.14 |

9.1.3 Released Files and Download Processes

| Function | Files | Carrier | Modem Firmware | MCU Firmware | Linux Distribution | Base Legato System |
|---|------------------------------|--------------------|----------------------|--------------|----------------------|--------------------|
| WP7702 Approved | | | | | | |
| Windows one-click firmware upgrade tool | WP77xx_Release 9_TMOBILE.exe | GENERIC (T-Mobile) | SWI9X06Y_02.13.02.00 | 002.009 | SWI9X06Y_02.16.02.00 | 18.03.0 |
| Test | | | | | | |
| Windows one-click firmware upgrade tool | WP77xx_Release 9_GENERIC.exe | GENERIC | SWI9X06Y_02.16.04.00 | 002.009 | SWI9X06Y_02.16.02.00 | 18.03.0 |
| | WP77xx_Release 9_ATT.exe | ATT | SWI9X06Y_02.16.04.00 | 002.009 | SWI9X06Y_02.16.02.00 | 18.03.0 |
| | WP77xx_Release 9_VERIZON.exe | VERIZON | SWI9X06Y_02.16.04.00 | 002.009 | SWI9X06Y_02.16.02.00 | 18.03.0 |
| | WP77xx_Release 9_TELSTRA.exe | TELSTRA | SWI9X06Y_02.16.04.00 | 002.009 | SWI9X06Y_02.16.02.00 | 18.03.0 |
| From: https://source.sierrawireless.com/resources/airprime/software/wp77xx/wp77xx-firmware-release-9 | | | | | | |

| Function | Files |
|---|--|
| Firmware Components | 9999999_9907618_SWI9X06Y_02.13.02.00_00_GENERIC_001.009_000.spk (T-Mobile) 9999999_9907618_SWI9X06Y_02.16.04.00_00_GENERIC_001.021_000.spk (GCF) 9999999_9907787_SWI9X06Y_02.16.04.00_00_ATT_001.019_000.spk 9999999_9908088_SWI9X06Y_02.16.04.00_00_VERIZON_001.009_000.spk 9999999_9908397_SWI9X06Y_02.16.04.00_00_TELSTRA_001.004_000.spk linux-SWI9X06Y_02.16.02.00.cwe legato-18.03.0.cwe mcfw_002.009_wp77_f1.cwe |
| From: https://source.sierrawireless.com/resources/airprime/software/wp77xx/wp77xx-firmware-release-9 | |

| | | | |
|-------------|---------|-----------|-------|
| Template #: | 4124005 | Revision: | 01.06 |
|-------------|---------|-----------|-------|

9.2 Software Changes Description

The WP77xx Release 9, based on modem version SWI9X06Y_02.16.04.00, is functionally equivalent to WP76xx Release 9 [5], with notable differences and features below.

| ID | Title | Description | Impacted Domain |
|--------------|---|---|-------------------------------|
| Legato | | | |
| Various | Legato 18.03.0 | Legato 18.03.0 http://legato.io/legato-docs/latest/releaseNotes18030.html http://legato.io/legato-docs/latest/releaseNotes18020.html Upgrade from 18.01.0 in Release 8 | Legato AF |
| Modem | | | |
| Core | | | |
| QT19X07-2016 | Add Qualcomm MDM9206.LE.2.0-00122-STD.PROD-1.149002.1 | Adds Qualcomm baseline MDM9206.LE.2.0-00122-STD.PROD-1.149002.1 | Qualcomm baseline (Release 9) |
| System | | | |
| QT19X07-1813 | WP77 crash during download package using X-modem | When attempting to perform XMODEM firmware download firmware over the modem USB AT port or the UART port, the device will crash every time. This feature is now fixed and supported. | Firmware Update |
| AT commands | | | |
| QT19X07-1984 | [WP77] SELMODE returns wrong setting | When selecting system mode via AT!SELMODE, the setting is not written into the device non-volatile memory and unable to persist across power cycles. | AT/SD |
| QT19X07-1697 | AT!BAND? returns Unknown Band | The device band mask will become shown as "Unknown" if the device changes between different RATs. | AT/SD |
| QMI | | | |
| QT19X07-1460 | QMI_NAS_GET_CELL_LOCATION_INFO_REQ_MSG_V01 return error | Legato application and AVMS server was unable to retrieve the device's current cell location ID via QMI because the feature to report modem data statistics was disabled on this chipset. This feature has now been enabled, and the QMI command is working as expected to report the cell location ID. | QMI/NAS |
| Data | | | |
| QT19X07-2015 | [WP77] SWI Proxy not working | The feature to set Data Bridge Mode was disabled on the 9x06 chipset by default, causing the modem and Legato application to unable to share a data connection. This feature has been enabled and PDN data multiplexing is now supported. | Data Connectivity |
| QT19X07-1917 | [WP77] Re-enable TLS 1.2 in SO Task | Originally, the mdm9x06 chipset only supported TLS 1.1 for secure sockets. Now that TLS 1.2 support is added, this change will update the device to use TLS 1.2 by default. | Security |
| RF | | | |

| ID | Title | Description | Impacted Domain |
|----------------|--|---|-----------------|
| QT19X07-1779 | GSM Multislot Class BLER Failure | High BLER is observed on GSM low bands when using multiple slots on the downlink. The ASM switching timing was increased in the RF Driver to resolve this issue. | RF/Driver |
| QT19X07-1948 | [WP77] Update Default LTE Power Backoff RF NVs | LTE B2, B5, B12, B13, B26 power backoff NVs were updated to pass FCC certification. | RF/Cal |
| Network Access | | | |
| QT19X07-1852 | [WP7702][36.523-1][22.3.2.1][NB-IOT] AM RLC | NB-IOT UE RLC sets the poll bit in all RLC PDUs, which is not expected for GCF testing, but done to provide better data rate. The poll bit should not be set for all RLC PDU, instead it should only be set for the ones configured by the network. | NAS/Protocol |
| Config | | | |
| QT19X07-1955 | Add NV psm_config_ext to EFSCconfig XML and persistence list | The PSM sleep duration was adjusted to compensate for the device's boot-up time for better timing accuracy when performing the TAU with the network on wake up. | PSM |
| QT19X07-1236 | [WP7702][AT&T][LTE-CM1-4-6907] - CAT M - MO SMS wakes UE from PSM | The device was a few seconds delayed in performing the TAU with the network after waking up from PSM due to long boot up time. This was fixed by adjusting the PSM sleep duration to compensate for the boot up time. | PSM |
| QT19X07-1249 | [WP7702][AT&T][LTE-CM1-4-6908] - CAT M - MO DATA wakes UE from PSM | The device was a few seconds delayed in performing the TAU with the network after waking up from PSM due to long boot up time. This was fixed by adjusting the PSM sleep duration to compensate for the boot up time. | PSM |

9.3 Known Issues

This section presents all known issues in this release.

| ID | Title | Description | Impacted Domain |
|--------------|--|---|-----------------|
| Bugs | | | |
| QT19X07-1308 | Missing Java dependency for building LK bootloader | The Android Signing tools for the LK bootloader require Java Runtime Environment (JRE) to be installed on the host platform. JRE has not been added to the build environment, so must be installed on the build machine manually. Example, for Ubuntu 16.04: sudo apt-get install default-jre | Build |
| QT19X07-1293 | Current consumption – UART1 with AT+KSLEEP=1 | If UART1 is mapped to AT commands with AT+KSLEEP=1 AND there is a physical UART connected , the module consumes an average of ~10mA in idle and LPM modes. | Power |

| ID | Title | Description | Impacted Domain |
|-----------------------------|---|---|-----------------|
| QT19X07-959 QT19X07-1121 | Deficiencies in GPIO control from linux | While fixed in modem (see Release 7), certified images (PTCRB, AT&T, Verizon: SWI9X07Y_02.10.xx.00) do not benefit. A <i>new</i> linux patch for older modem versions has been simplified from the previous release. No configuration changes are required so future upgrades will work without reverting configuration. Reference DAYTONA-8683 for patch available from your Sierra support contact. | GPIO |
| QT19X07-1007 | PCM configuration not allowed by default | The ability to set a profile to use a particular interface is controlled by AT!AVPIFACEPREF (level 2 access). By default, PCM was not included so PCM could not be set with AT!AVCFG without first setting AT!AVPIFACEPREF=F. The factory default has been updated to make PCM available by default, however this will only benefit newly manufactured units so AT!AVPIFACEPREF=F is still required. | Audio |
| QT19X07-1494 | Legato - boot loop error when built with large database | Customer legato.cwe image must be small enough to fit into the LEFWKRO partition (8MB). | Legato |

10 SWI9X06Y Release 8

Release 8 is intended as a certification refresh candidate to resolve several issues for carrier and industrial certification testing. It is important to note that:

- No GCF and PTCRB certification has been granted yet.
- AirVantage and FOTA now has basic functionality

10.1 Software Release Description

10.1.1 Release identification

| Component | Revision |
|------------------------------|--|
| Modem Firmware | SWI9X06Y_02.14.04.00 a03347 jenkins 2018/02/19 06:13:56 |
| Linux Firmware | SWI9X06Y_02.14.04.00 2018-02-19_00:48:31 |
| MCU Firmware | 002.007 |
| Legato Application Framework | 18.01.0_7946ce7181b7425bad75f7086b992e9b |
| Binary Size | 50MB (compressed binaries) |
| IMEI SV | 2 |
| Qualcomm Stack Version | MDM9206.LE.2.0-00115-STD.PROD-1 |
| Linux Kernel Version | Linux version 3.18.44 (jenkins@jenkins) (gcc version 6.2.0 (GCC)) #2 PREEMPT Mon Feb 19 01:13:41 UTC 2018 |
| Supported H/W | WP7702 DV1.1+ WP7700 DV 2.1+ |



10.1.2 Software Tools Versions

| S/W Tools Name | Version |
|------------------------|--------------|
| Windows Driver Package | B4773 |
| Windows SDK | None |
| Skylight | None |
| Linux Drivers | S2.31N2.49 |
| Linux SDK | SLQS04.00.12 |

10.1.3 Released Files and Download Processes

| Function | Files | Carrier | Modem Firmware | MCU Firmware | Linux Distribution | Base Legato System |
|---|------------------------------|-----------------------------|----------------------|--------------|----------------------|--------------------|
| Windows one-click firmware upgrade tool | WP77xx_Release 8_TMOBILE.exe | GENERIC (T-Mobile) | SWI9X06Y_02.13.02.00 | 002.007 | SWI9X06Y_02.14.04.00 | 18.01.0 |
| | WP77xx_Release 8_GENERIC.exe | GENERIC (GCF, not approved) | SWI9X06Y_02.14.04.00 | 002.007 | SWI9X06Y_02.14.04.00 | 18.01.0 |
| | WP77xx_Release 8_ATT.exe | ATT (not approved) | SWI9X06Y_02.14.04.00 | 002.007 | SWI9X06Y_02.14.04.00 | 18.01.0 |

From: <https://source.sierrawireless.com/resources/airprime/software/wp77xx/wp77xx-firmware-release-8>

| Function | Files |
|---------------------|---|
| Firmware Components | 9999999_9907618_SWI9X06Y_02.14.04.00_00_GENERIC_001.012_000.spk (GCF) 9999999_9907618_SWI9X06Y_02.13.02.00_00_GENERIC_001.009_000.spk (T-Mobile) 9999999_9907787_SWI9X06Y_02.14.04.00_00_ATT_001.011_000.spk linux-SWI9X06Y_02.14.04.00.cwe legato-18.01.0.cwe mcufw 002.007 wp77 f1.cwe |

From: <https://source.sierrawireless.com/resources/airprime/software/wp77xx/wp77xx-firmware-release-8>

10.2 Software Changes Description

The WP77xx Release 8, based on modem version SWI9X06Y_02.14.04.00, is functionally equivalent to WP76xx Release 8 [5], with notable differences and features below.

| ID | Title | Description | Impacted Domain |
|---------|----------------|---|-----------------|
| Legato | | | |
| Various | Legato 18.01.0 | Legato 18.01.0 http://legato.io/legato-docs/latest/releaseNotes18010.html Upgrade from Legato 17.11.0 in Release 7 | Legato AF |
| Modem | | | |
| Core | | | |

| ID | Title | Description | Impacted Domain |
|--------------|---|---|-------------------------------|
| QT19X07-1497 | Add Qualcomm MDM9206.LE.2.0-00115-STD.PROD-1 | Adds Qualcomm baseline MDM9206.LE.2.0-00115-STD.PROD-1 | Qualcomm baseline (Release 8) |
| QT19X07-1591 | Increment IMEI SV to 2 | IMEI SVN was incremented to 2 for this release | System |
| AT commands | | | |
| QT19X07-583 | Add support to select between LTE CAT-M1 and CAT-NB1 RATs | AT!SELCIOT was introduced to allow user to select between LTE CAT-M1 and CAT-NB1 operating modes | AT/SD |
| QT19X07-1210 | [WP77] Add AT command to set SNR scan level to optimize NB1 scanning time on eMTC | AT!SELSNR was introduced to allow user to configure the depth of scan on LTE NB1 networks to optimize scanning time | AT/SD |
| QMI | | | |
| QT19X07-1436 | WP7702 failed to retrieve data for Location object (lwm2m.6.0.x) with error "Resource does not exist" | Fixes an issue where the Position Report indication from the LOC engine is not being sent to inactive clients. | QMI/NAS |
| RF | | | |
| QT19X07-1540 | Update GSM Max Power Level NVs | GSM Max Power Level NVs were updated to pass FCC certification and to stay consistent with WPx5xx Antenna Gain settings | RF/NV |
| QT19X07-1285 | [WP77] RFCal Verification Failures on eMTC | Fixes numerous issues seen during LTE CAT-M1 RF Calibration Verification at factory | RF/Cal |

10.3 Known Issues

This section presents all known issues in this release.

| ID | Title | Description | Impacted Domain |
|----------|--|--|-----------------|
| Features | | | |
| Various | AirVantage Connectivity | AirVantage Connectivity now has basic functionality. Full validation is still being performed. | AirVantage |
| Various | FOTA | FOTA support has been implemented and has basic functionality. Full validation is still being performed. | FOTA |
| Bugs | | | |
| LE-7418 | avcControl will block other data connections from using that APN | If the Legato AirVantage connector has a connection established, any other data connect to that APN is blocked. Conversely if a data connection is already established on that APN, the Legato AirVantage connector cannot connect. <i>The resolution is currently undergoing full testing for delivery in Release 9.</i> | Networking |

| ID | Title | Description | Impacted Domain |
|--------------|---|---|-------------------|
| LXSWIREF-273 | Re-building kernel fails with Yocto 2.2 due to "metadata not deterministic" error | Every kernel build from the source distribution must be built from clean or before each kernel re-build, execute the following: touch meta-swi/meta-swi-mdm9x28/recipes-kernel/linux/linux-quic_git.bb | Build |
| QT19X07-1308 | Missing Java dependency for building LK bootloader | The Android Signing tools for the LK bootloader require Java Runtime Environment (JRE) to be installed on the host platform. JRE has not been added to the build environment, so must be installed on the build machine manually. Example, for Ubuntu 16.04: sudo apt-get install default-jre | Build |
| QT19X07-599 | Sierra SIM Connectivity | AT+COPS=2 shall NOT be used with this module to trigger any network steering | Connectivity |
| DAYTONA-8511 | UART1 does not wake up on Rx | After a few seconds of idle time the UART enters a state of runtime suspend after which time serial activity from the host cannot wake the module to receive. This issue was introduced in Release 7. A patch to the linux distribution is available | UART |
| QT19X07-780 | Current consumption and data throughput – HSIC enabled | The module will not enter sleep mode if HSIC is enabled, and the host platform does not have an HSIC (ethernet) controller connected . Minimum power consumption while not in sleep mode is ~40mA. This has also been found to increase CPU loading and consequently CAT4 max downlink throughput is degraded in some cases. For platforms without a HSIC controller, this feature should be disabled with AT!CUSTOM="HSICENABLE",0 | Power, Throughput |
| QT19X07-1293 | Current consumption – UART1 with AT+KSLEEP=1 | If UART1 is mapped to AT commands with AT+KSLEEP=1 AND there is a physical UART connected , the module consumes an average of ~10mA in idle and LPM modes. | Power |
| QT19X07-1001 | Current consumption in PSM mode | Current consumption is not optimized in PSM mode. Significant improvements are planned for the next release. See Software Changes Description for the WP76xx Release 8 [5] . ULPS mode is not affected. | Power/PSM |

11 SWI9X06Y Release 7

Release 7 is provided for customer samples to demonstrate initial PSM support, and is intended to resolve a number of issues for carrier and industrial certification testing. It is important to note that:

- Legato Application Framework is supported, but limited validation has been performed
- No formal GCF, PTCRB or Carrier certification testing has been performed.
- Linux Firmware source code will not be published to Source
- AirVantage and FOTA are not supported

11.1 Software Release Description

11.1.1 Release identification

| Component | Revision |
|------------------------------|--|
| Modem Firmware | SWI9X06Y_02.13.02.00 7cfe8a jenkins 2017/12/22 05:21:50 |
| Linux Firmware | SWI9X06Y_02.13.02.00 2017-12-22_06:09:25 |
| MCU Firmware | 002.006 |
| Legato Application Framework | 17.11.0_3238a5a8f17311821611a475aba506b4 |
| Binary Size | 50MB (compressed binaries) |
| IMEI SV | 1 |
| Qualcomm Stack Version | MDM9206.LE.2.0-00109-STD.PROD-1 |
| Linux Kernel Version | Linux version 3.18.44 (jenkins@jenkins) (gcc version 6.2.0 (GCC)) #2 PREEMPT Fri Dec 22 06:18:41 UTC 2017 |
| Supported H/W | WP7702 DV1.1+ WP7700 DV 2.1+ |

11.1.2 Software Tools Versions

| S/W Tools Name | Version | |
|------------------------|--------------|--|
| Windows Driver Package | B4773 | |
| Windows SDK | None | |
| Skylight | None | |
| Linux Drivers | S2.31N2.49 | Important upgrade required for multi RMNET support. |
| Linux SDK | SLQS04.00.11 | |

11.1.3 Released Files and Download Processes

Release 7 is provided as programmed hardware samples only. Software update packages are available upon request, and is not distributed on Source.

| Function | Files | Carrier (not approved) | Modem Firmware | MCU Firmware | Linux Distribution | Base Legato System |
|---|------------------------------|---------------------------|----------------------|--------------|----------------------|--------------------|
| Windows one-click firmware upgrade tool | WP77xx_Release 7_GENERIC.exe | GENERIC | SWI9X06Y_02.13.02.00 | 002.006 | SWI9X06Y_02.13.02.00 | 17.11.0 |
| | WP77xx_Release 7_ATT.exe | ATT | SWI9X06Y_02.13.02.00 | 002.006 | SWI9X06Y_02.13.02.00 | 17.11.0 |
| Linux SPK files | WP77xx_Release 7_GENERIC.spk | GENERIC | SWI9X06Y_02.13.02.00 | 002.006 | SWI9X06Y_02.13.02.00 | 17.11.0 |
| | WP77xx_Release 7_ATT.spk | ATT | SWI9X06Y_02.13.02.00 | 002.006 | SWI9X06Y_02.13.02.00 | 17.11.0 |

11.2 Software Changes Description

The WP77xx Release 7, based on modem version SWI9X06Y_02.13.02.00, is functionally equivalent to WP76xx Release 7 [\[5\]](#), with notable differences and features below.

| ID | Title | Description | Impacted Domain |
|--------------|--|---|-------------------------------|
| Legato | | | |
| Various | Legato 17.11.0 | Legato 17.11.0 http://legato.io/legato-docs/latest/releaseNotes17110.html http://legato.io/legato-docs/latest/releaseNotes17100.html http://legato.io/legato-docs/latest/releaseNotes17090.html Upgrade from Legato 17.08.1 in Release 6 | Legato AF |
| LE-7907 | Legato APIs to support 3GPP eDRX (specification) | Adds support for Legato APIs used to configure eDRX | Legato, LPWA |
| Modem | | | |
| Core | | | |
| QT19X07-1191 | Add Qualcomm MDM9206.LE.2.0-00109-STD.PROD-1 | Adds Qualcomm baseline MDM9206.LE.2.0-00109-STD.PROD-1 | Qualcomm baseline (Release 7) |
| Various | eDRX | eDRX is supported. Legato API support have also been added. | LPWA |
| N/A | Extended Coverage | Extended Coverage mode A on LTE CAT M1 is supported but not tested. Pending validation during industrial certification | LPWA |
| Data | | | |
| QT19X07-608 | [WP7702] Consecutive data connection doesn't work using SLQS | Fixes the issue where user is unable to start a second consecutive data connection on Linux without resetting the device | DATA |
| AT commands | | | |
| QT19X07-1259 | Add LTE CAT M1 and CAT NB1 into ATISELACQ | Adds support to allow user to configure the network acquisition order between LTE CAT M1, CAT NB1, and GSM to optimize scanning times. Currently, the user cannot set the preference of CAT M1 and NB1 networks separately. | AT |
| QT19X07-1223 | [9x06] Restore +CNUM, \$QCPBMPREF AT commands | Re-enables AT+CNUM ad \$QCPBMPREF AT commands | AT |
| QT19X07-1274 | [WP7702][AT&T][LTE-FLD-2-1502] - LTE Normal MM Detach From Idle Mode | Fixes an issue where AT+COPS=0 will return "SIM ERROR" after executing AT+COPS=2 | AT |
| QT19X07-1161 | Incorrect RAT reported in AT+COPS on Cat-M1 | Corrects the RAT displayed in AT+COPS output on LTE CAT-M1 network | AT |
| QMI | | | |
| QT19X07-1264 | QMI_NAS_GET_TECHNOLOGY_PREFERENCE disabled in 9x06 build | Re-enables the following QMI commands to allow host to set RAT preference on the device: - QMI_NAS_GET_TECHNOLOGY_PREFERENCE - QMI_NAS_SET_TECHNOLOGY_PREFERENCE | QMI/NAS |
| QT19X07-1123 | [Unknown SIM State] on WP7702 | Re-enables the QMI CAT service to handle Legato SIM management APIs | QMI/CAT |
| RF | | | |
| QT19X07-1328 | Update GSM backoff default NVs | Introduces GSM multi slot backoff for power consumption savings | RF/NV |
| QT19X07-1329 | GNSS Desense in LTE CATM Traffic | Adds GNSS Blanking to LTE Bands to reduce GNSS desense | RF/Driver |

| | | | |
|-------------|---------|-----------|-------|
| Template #: | 4124005 | Revision: | 01.06 |
|-------------|---------|-----------|-------|

| ID | Title | Description | Impacted Domain |
|--------------|---|--|-----------------|
| QT19X07-1159 | Default NV update, GSM Timing, LIMIT_VS_TEMP | Updates the default static NVs for GSM Timing and Limit vs. Temperature data | RF/NV |
| QT19X07-1049 | Crash during RF Cal/ Verification on Non-Signalling calls | Fixes a crash seen during LTE CATM RFCAL verification in non-signaling mode | RF |
| QT19X07-1135 | Make GSM PA optional for WP7700 HW | Removes GSM PA scanning on RFFE bus for WP7700 HW to fix the issue where device will be stuck in Factory Test Mode | RF/Driver |
| QT19X07-1271 | Remove B39 from default band mask | Qualcomm has removed LTE TDD support on this chipset, so B39 support has been removed | RF/Driver |

11.3 Known Issues

This section presents all known issues in this release.

| ID | Title | Description | Impacted Domain |
|-----------------|---|--|-----------------|
| Features | | | |
| Various | AirVantage Connectivity | AirVantage is not supported | AirVantage |
| Various | FOTA | FOTA is not supported | FOTA |
| Various | Partial AT support | This release does not support all planned AT commands. | AT |
| Various | PSM | PSM is supported in this release. Current consumption is still yet to be optimized. | LPWA |
| QT19X07-1210 | Long scanning time on LTE CAT NB1 networks | <p>By Qualcomm's design, the UE will take an extended period of time (up to 20 minutes, may be even longer depending on network conditions) to scan for cells on the LTE NB1 network during the first initial attach. This will take even longer if there is no NB1 service available.</p> <p>In the case when there's no NB1 network, the user can use AT!SELACQ to set LTE-NB1 RAT to a lower priority so the NB1 cells are not scanned before CAT M1 and GSM.</p> | Network Access |
| Bugs | | | |
| LE-7418 | avcControl will block other data connections from using that APN | If the Legato AirVantage connector has a connection established, any other data connect to that APN is blocked. Conversely if a data connection is already established on that APN, the Legato AirVantage connector cannot connect. | Networking |
| LXSWIREF-273 | Re-building kernel fails with Yocto 2.2 due to "metadata not deterministic" error | Every kernel build from the source distribution must be from clean or before each kernel re-build, execute the following: touch meta-swi/meta-swimdm9x28/recipeskernel/linux/linux-quic_gjit.bb | Build |

| ID | Title | Description | Impacted Domain |
|------------------------------|---|--|------------------|
| LXSWIREF-248 | UBIFS: User partition corruption after number of power cuts | If power is cut suddenly, it is possible that data will be wiped out from UBIFS partition mounted @ /mnt/flash mount point. | Linux Filesystem |
| QT19X07-583 | AT!SELRAT support for LTE CAT-M1 and CAT-NB1 | AT!SELRAT currently cannot be used for RAT selection between LTE CAT-M1 and CAT-NB1 networks. It can only be used to select between GSM and LTE. Please use AT!SELACQ for setting RAT preference in the meantime. | Network Access |
| QT19X07-1322 | WP modules boot into low power mode | If W_DISABLE feature is enabled (via AT!PCOFFEN), some hardware platforms (depending on line capacitance) may observe that this condition is incorrectly triggered on power up and the module stays in low power mode (radio off). To confirm if this is the case use at!pinfo? to check if W_DISABLE is the condition holding the module in low power mode. | RF |
| QT19X07-599 | Sierra SIM Connectivity | AT+COPS=2 shall NOT be used with this module to trigger any network steering | Connectivity |
| QT19X07-780 | Current consumption – HSIC Enabled | The module will not enter sleep mode if HSIC is enabled, but host platform does not have ethernet controller connected. Minimum power consumption while not in sleep mode is ~40mA. | Power |
| QT19X07-1224 QT19X07-1225 | Current consumption – UART1 mapped to AT | If UART1 is mapped to AT commands, the module consumes an average of ~10mA in idle and lpm modes. | Power |
| QT19X07-1001 | Current consumption in PSM mode | Current consumption is higher than expected in PSM mode because I2C bus is enabled | Power/PSM |
| QT19X07-959 QT19X07-1121 | Deficiencies in GPIO control from linux | While fixed in modem (see above), certified images do not benefit. There is, however, a workaround for older modem versions. 1) Configure desired GPIOs in AT+WIOCFG with function=0 e.g. AT+WIOCFG=13,0 2) Remove the following lines from kernel/drivers/gpio/gpiolib-sysfs.c | GPIO |
| QT19X07-1128 | GPSREFLOC customization support | Customization to report reference location in NMEA stream is not supported | GNSS |
| LXQMIDRV-216 | Linux SDK | Tethered Linux host may freeze during suspend/resume stress testing | Drivers |

12 SWI9X06Y Release 6

Release 6 is provided for initial customer samples and is intended to be the initial firmware candidate for carrier and industrial certification testing. It is important to note that:

- Legato Application Framework is not fully supported
- No formal GCF, PTCRB or Carrier certification testing has been performed.
- Linux Firmware source code will not be published to Source

| | | | |
|-------------|---------|-----------|-------|
| Template #: | 4124005 | Revision: | 01.06 |
|-------------|---------|-----------|-------|

- AirVantage and FOTA are not supported

12.1 Software Release Description

12.1.1 Release identification

| Component | Revision |
|------------------------------|--|
| Modem Firmware | SWI9X06Y_02.09.02.00 d875da jenkins 2017/10/22 22:48:21 |
| Linux Firmware | SWI9X06Y_02.09.02.00 2017-10-22_23:00:42 |
| MCU Firmware | 002.004 |
| Legato Application Framework | 17.08.1_c073924cf80081f79fd125fae2f0d6cf |
| Binary Size | 54MB (compressed binaries) |
| IMEI SV | 1 |
| Qualcomm Stack Version | MDM9206.LE.2.0-00103-STD.PROD-1 |
| Linux Kernel Version | Linux version 3.18.44 (jenkins@jenkins) (gcc version 4.9.1 (GCC)) #2 PREEMPT Sun Oct 22 23:14:48 UTC 2017 |
| Supported H/W | WP7702 DV1.1+ |

12.1.2 Software Tools Versions

| S/W Tools Name | Version | Resource file |
|------------------------|----------------|---------------|
| Windows Driver Package | B4762 | |
| Windows SDK | None | |
| Skylight | None | |
| Linux Drivers | S2.29N2.44 | |
| Linux SDK | SLQS04.00.10.1 | |

12.1.3 Released Files and Download Processes

Release 6 is provided as programmed hardware samples only. Software update packages are available upon request, and is not distributed on Source.

| Download Option | Files |
|-----------------|----------------------------------|
| Windows | WP77xx_Release6_GENERIC_test.exe |
| SPK files | WP77xx_Release6_GENERIC_test.spk |

12.2 Software Changes Description

The WP77xx Release 6, based on modem version SWI9X06Y_02.09.02.00, is functionally equivalent to WP76xx Release 6 [\[5\]](#), with notable differences and features below.

| ID | Title | Description | Impacted Domain |
|--------|-------|-------------|-----------------|
| Legato | | | |



| ID | Title | Description | Impacted Domain |
|-------------|--|---|-------------------------------|
| Various | Legato 17.08.1 | Legato 17.08.1 http://legato.io/legato-docs/latest/releaseNotes17081.html | Legato AF |
| Modem | | | |
| Core | | | |
| QT19X07-991 | Add Qualcomm MDM9206.LE.2.0-00103-STD.PROD-1 | Add Qualcomm MDM9206.LE.2.0-00103-STD.PROD-1 | Qualcomm baseline (Release 6) |
| HW variants | | | |
| Various | WP77xx support added | BSP and RF driver support was added for WP7702 and WP7700. | RF/BSP |

12.3 Feature Notes

12.3.1 Multi RMNET vs. QMAP

In previous generation devices, multiple RmNet interfaces were supported through dedicated BAM channel interfaces, configured via USB composition. This approach imposed a limit on the number of interfaces that could be simultaneously supported. To remove that limitation, QMAP was introduced to multiplex multiple virtual channels over a single interface. To make use of this feature, the number of interfaces must be set (AT!NETNUM) and new host drivers are required (S2.29N2.47 or later). Note, however, that in moving to multiple RmNet with QMAP only a single dedicated channel is supported. If only a single RmNet is required, operation in non QMAP mode (AT!NETNUM=0) is still supported with older drivers (S2.29N2.44).

See SLQS04.00.10.1 release package for more details. QMAP is not supported by the Windows driver, and only one RmNet interface will be exposed regardless of AT!NETNUM setting.

12.3.2 Voice/VoLTE

This commercial release does not support Audio, Voice or VoLTE.

12.4 Known Issues

This section presents all known issues in this release.

| ID | Title | Description | Impacted Domain |
|----------|-------------------------|--|-----------------|
| Features | | | |
| Various | AirVantage Connectivity | AirVantage is not supported | AirVantage |
| Various | FOTA | FOTA is not supported | FOTA |
| Various | Partial AT support | This release does not support all planned AT commands. | AT |
| Various | PSM | PSM is not supported in this Release. | LPWA |
| Various | eDRX | eDRX is supported on the protocol level, but current consumption needs to be optimized. | LPWA |
| N/A | Extended Coverage | Extended Coverage mode A on LTE CAT M1 is supported but not tested. Pending validation during industrial certification | LPWA |

| ID | Title | Description | Impacted Domain |
|--------------|--|--|-----------------|
| Various | Linux Boot time is not optimized | <p>Various debug capabilities and debug modules are included in the Kernel and Rootfs, which increases the Sierra Linux system boot time.</p> <p>Modem communication interfaces initialize after the kernel is started, and a delay is observed between USB enumeration and functional communication on the USB interfaces such as the Network adapter, Modem port, etc. Delays of approximately 5 seconds are measured on typical power up, and up to 25 seconds when Linux is starting up for the first time on blank flash.</p> | Linux / Boot |
| Bugs | | | |
| QT19X07-608 | Consecutive Data Connection on Linux | On a Linux host, user is currently only able to make one data connection after boot up. The device needs to be reset if the first call is disconnected from the host and a second data connection is required. This does not affect Windows users. | Connectivity |
| QT19X07-583 | RAT selection and acquisition order for LTE CAT-M1 and CAT-NB1 | There is currently no AT command to select RAT preference between LTE CAT M1 and NB1. The device will by default search for CAT M1 network first, and then NB1. | Network Access |
| LXSWIREF-211 | Legato ECM Interface | ECM MAC address on the host doesn't match the WP for linux kernel 4.4.x hosts (e.g. Ubuntu 14.04 / 16.04) Note: This will be fixed in the next release. | USB / ECM |
| QT19X07-599 | Sierra SIM Connectivity | AT+COPS=2 shall NOT be used with this module to trigger any network steering | Connectivity |
| QT19X07-310 | Data from the UE to the DHCP server failed | When customization DHCPRELAYENABLE is enabled, allow only UDP packets for port 67 with target IP address 0xFFFFFFFF to be filtered to the internal DHCP server on modem. All others are sent to the air interface. Note: This will be fixed in the next release. | DHCP |
| QT19X07-780 | Current consumption | <p>The module will not enter sleep mode if:</p> <ol style="list-style-type: none"> 1) HSIC is enabled, but host platform does not have ethernet controller connected. 2) Module is booted without USB connected, unless USB is subsequently connected. <p>Minimum power consumption while not in sleep mode is ~40mA. PSM is not yet supported, however ULPS is.</p> | Power |
| QT19X07-959 | GPIO24 defaults to high after exporting | Upon initial export of GPIO24 from sysfs it is initially high rather than input, no pull | GPIO |
| QT19X07-995 | Unable to get MS-Assisted GPS fix in some cases. | Device rejecting server SSL certificate because the key length is smaller than the minimum value. Pending Qualcomm CR 978483 | GNSS |

13 Troubleshooting

Please contact customer service for support and debug

14 Certification Description

Release 6 is not intended for customer use as industrial or carrier certification candidates.

15 Restrictions and Additional Information

This section presents additional information or restrictions that must be taken into account.

| ID | Description (What/When) | Impacted Domain |
|---------|---|-----------------|
| Various | Modules should not be used on live networks | Certification |