SIERRA WIRELESS IS NOW SEMTECH®

Modules

Customer Release Notes

EM929x

Apr 08, 2026

41114778 Rev. 1.20.4

Revision History

Rev#	Date (YYYY/MM/DD)	Updates
1.01	2022/09/20	Release 1 BP4
1.02	2022/11/06	Release 1 BP5
1.03	2022/12/14	Release 1 BP6
1.03.1	2022/12/20	Amended Linux FW update instructions
1.04	2023/02/15	Release 1 BP7
1.05	2023/03/24	Release 1 BP8
1.06	2023/04/26	Release 1 BP9
1.07	2023/06/15	Release 1 BP10
1.08	2023/07/26	Release 1 BP11
1.09	2023/08/29	Release 1 BP12
1.10	2023/09/29	Release 1 BP13
1.11	2023/10/17	Release 1 commercial release. Removed all pre-commercial releases.
1.12	2023/12/08	Release 2
1.12.01	2024/01/30	Release 2.1
1.13	2024/04/10	Release 3
1.14	2024/05/24	Release 4
1.15	2024/05/29	Release 5
1.16	2024/07/18	Release 6
1.17	2024/12/03	Release 6.1
1.18	2025/02/03	Release 7
1.19	2025/04/23	Release 6.2
1.20	2025/05/29	Release 8
1.20.1	2025/10/31	Release 8 - Updated for PCTRB, Bell, VZW and Rogers certification approval Updated for VoNR disabled note.
1.20.2	2025/12/16	Release 8 – Updated for DOCOMO, KDDI, SOFTBANK certification approval
1.20.3	2026/02/10	Release 8 – Updated for ATT, TMO certification approval. And VZW PRI ver for carrier policy fix.
1.20.4	2026/04/08	Release 8 – Updated for Telus certification approval. And VZW PRI ver for failure manager configs.

Contents

CONTENTS 3
1 INTRODUCTION 7
1.1 Document Scope 7
1.2 Firmware Packages and Tools 7
1.3 Document Audience 7
2 COMPATIBILITY 8
2.1 Hardware compatibility 8
2.2 Software feature compatibility 8
3 FIRMWARE RELEASE 8 9
3.1 Firmware Release Description 9
3.1.1 Firmware Release Identification 9
3.1.2 Carrier Packages 9
3.1.3 Host Software Versions 11
3.1.4 Software Changes 11
3.1.5 Security Corrections/Improvements 13
3.1.6 Known Issues 14
4 FIRMWARE RELEASE 7 14
4.1 Firmware Release Description 15
4.1.1 Firmware Release Identification 15
4.1.2 Carrier Packages 15
4.1.3 Host Software Versions 16
4.1.4 Software Changes 17
4.1.5 Security Corrections/Improvements 18
4.1.6 Known Issues 19
5 FIRMWARE RELEASE 6.2 20

5.1 Firmware Release Description 20
5.1.1 Firmware Release Identification 20
5.1.2 Carrier Packages 20
5.1.3 Host Software Versions 22
5.1.4 Software Changes 22
5.1.5 Security Corrections/Improvements 23
5.1.6 Known Issues 23
6 FIRMWARE RELEASE 6.1 25
6.1 Firmware Release Description 25
6.1.1 Firmware Release Identification 25
6.1.2 Carrier Packages 25
6.1.3 Host Software Versions 26
6.1.4 Software Changes 26
6.1.5 Security Corrections/Improvements 27
6.1.6 Known Issues 27
7 FIRMWARE RELEASE 6 28
7.1 Firmware Release Description 28
7.1.1 Firmware Release Identification 28
7.1.2 Carrier Packages 28
7.1.3 Host Software Versions 29
7.1.4 Software Changes 30
7.1.5 Security Corrections/Improvements 31
7.1.6 Known Issues 31
8 FIRMWARE RELEASE 5 33
8.1 Firmware Release Description 33
8.1.1 Firmware Release Identification 33
8.1.2 Carrier Packages 33
8.1.3 Host Software Versions 34

8.1.4 Software Changes 34
8.1.5 Security Corrections/Improvements 35
8.1.6 Known Issues 36
9 FIRMWARE RELEASE 4 37
9.1 Firmware Release Description 37
9.1.1 Firmware Release Identification 37
9.1.2 Carrier Packages 37
9.1.3 Host Software Versions 38
9.1.4 Software Changes 38
9.1.5 Security Corrections/Improvements 40
9.1.6 Known Issues 40
10 FIRMWARE RELEASE 3 42
10.1 Firmware Release Description 42
10.1.1 Firmware Release Identification 42
10.1.2 Carrier Packages 42
10.1.3 Host Software Versions 43
10.1.4 Software Changes 43
10.1.5 Security Corrections/Improvements 44
10.1.6 Known Issues 44
11 FIRMWARE RELEASE 2.1 46
11.1 Firmware Release Description 46
11.1.1 Firmware Release Identification 46
11.1.2 Carrier Packages 46
11.1.3 Host Software Versions 47
11.1.4 Software Changes 47
11.1.5 Security Corrections/Improvements 47
11.1.6 Known Issues 47
12 FIRMWARE RELEASE 2 49

12.1 Firmware Release Description 49
12.1.1 Firmware Release Identification 49
12.1.2 Carrier Packages 49
12.1.3 Host Software Versions 50
12.1.4 Software Changes 50
12.1.5 Security Corrections/Improvements 51
12.1.6 Known Issues 52
13 FIRMWARE RELEASE 1 54
13.1 Firmware Release Description 54
13.1.1 Firmware Release Identification 54
13.1.2 Carrier Packages 54
13.1.3 Host Software Versions 55
13.1.4 Software Changes 55
13.1.5 Security Corrections/Improvements 55
13.1.6 Known Issues 55
14 TROUBLESHOOTING 57
14.1 QXDM Logging 57
15 FIRMWARE PACKAGE DOWNLOAD PROCESS 58
15.1 Windows Host via USB/PCIe 58
15.2 Linux Host via USB / PCIe 58
16 RELATED DOCUMENTATION 59
17 ABBREVIATIONS AND DEFINITIONS 60

1 Introduction

1.1 Document Scope

This document describes the firmware releases for the EM929x product family, which includes EM9291 and EM9293., … and [device].

Semtech highly recommends migrating to new releases when available to take advantage of any security and stability improvements.

1.2 Firmware Packages and Tools

Module resources, including firmware packages, release notes, tools and other product documentation are published on The Source at https://source.sierrawireless.com and can be accessed via the device-specific page.

1.3 Document Audience

This Release Notes document may be distributed to all direct and indirect customers.

2 Compatibility

2.1 Hardware compatibility

The latest firmware release is compatible with commercial EM9291 and EM9293 hardware. There are no major known issues with pre-commercial hardware, but it is no longer actively tested or supported.

2.2 Software feature compatibility

The EM929x feature set is closely compatible with the EM919x. Refer to [1] EM92 Migration Guide*[1] EM92 Migration Guide* for a detailed comparison against the previous generation of products.

3 Firmware Release 8

Release 8 adds new features – 2 Antenna support, SA ULCA and Power Class 1.5. This will be candidate to start North American Carrier Certifications

For PRI details, see *[2] EM92xx PRI Customer Release Notes*.

3.1 Firmware Release Description

3.1.1 Firmware Release Identification

Table 1. Firmware Release Identification – Release 8

Component	Details
Firmware Version	SWIX65C_03.04.10.01
Date of generation (UTC)	18-Jun-2025
IMEI SV	11
GSMA TS.25	24-Feb-2025
Chipset Vendor Stack Version	MPSS.DE.4.0.c1-00452-OLYMPIC_GENALL_PACK-1.109079.2.114012.2
Supported HW	EM9291, EM9293

3.1.2 Carrier Packages

Table 2. Carrier Packages – Release 8

Carrier	Firmware	Configuration	Comment
Approved			
ATT	SWIX65C_03.04.10.01	040.025_003	Release 8
BELL	SWIX65C_03.04.10.01	040.023_001	Release 8
DOCOMO	SWIX65C_03.04.10.01	040.026_002	Release 8
GENERIC	SWIX65C_03.04.10.01	040.025_001	Release 8
KDDI	SWIX65C_03.04.10.01	040.032_001	Release 8
PTCRB	SWIX65C_03.04.10.01	040.023_001	Release 8
ROGERS	SWIX65C_03.04.10.01	040.022_001	Release 8
SOFTBANK	SWIX65C_03.04.10.01	040.026_001	Release 8 – EM9291 Only

TELSTRA	SWIX65C_02.17.08.00	030.022_002	Release 6.1
TELUS	SWIX65C_03.04.10.01	040.023_001	Release 8
TMO	SWIX65C_03.04.10.01	040.022_001	Release 8
VERIZON	SWIX65C_03.04.10.01	040.025_004	Release 8
Approved Legacy			
ATT	SWIX65C_02.17.08.00	030.094_003	Release 6.1
ATT	SWIX65C_02.15.01.00	030.059_000	Release 2
BELL	SWIX65C_02.17.08.00	030.018_003	Release 6.1 - Accepted by Bell for Platform Certification
BELL	SWIX65C_02.15.01.00	030.002_000	Release 2 - Accepted by Bell for Platform Certification
DOCOMO	SWIX65C_02.17.08.00	030.023_005	Release 6.1
GENERIC	SWIX65C_02.17.10.00	030.086_003	Release 6.2
GENERIC	SWIX65C_02.17.08.00	030.081_004	Release 6.1
GENERIC	SWIX65C_02.17.02.00	030.073_000	Release 5
GENERIC	SWIX65C_02.16.05.00	030.069_000	Release 4
GENERIC	SWIX65C_02.15.08.00	030.062_000	Release 3
GENERIC	SWIX65C_02.15.01.00	030.054_001	Release 2
GENERIC	SWIX65C_02.13.08.00	030.047_003	Release 1
KDDI	SWIX65C_02.17.10.00	030.023_003	Release 6.2
PTCRB	SWIX65C_02.17.08.00	030.077_003	Release 6.1
PTCRB	SWIX65C_02.15.01.00	030.050_001	Release 2
PTCRB	SWIX65C_02.13.08.00	030.045_003	Release 1
ROGERS	SWIX65C_02.17.08.00	030.033_003	Release 6.1
SOFTBANK	SWIX65C_02.17.10.00	030.027_006	Release 6.2 – EM9291 Only
TELUS	SWIX65C_02.17.08.00	030.028_004	Release 6.1
TMO	SWIX65C_02.17.08.00	030.042_003	Release 6.1
TMO	SWIX65C_02.15.01.00	030.017_000	Release 2
VERIZON	SWIX65C_02.17.08.00	030.092_003	Release 6.1
VERIZON	SWIX65C_02.16.05.00	030.077_000	Release 4
VERIZON	SWIX65C_02.15.08.00	030.068_001	Release 3
Test			
TELSTRA	SWIX65C_03.04.10.01	040.023_001	Release 8

3.1.3 Host Software Versions

The following tools were validated against this release.

Note: *Semtech recommends upgrading to newer Host Software releases when available. Refer to applicable software release notes for any compatibility restrictions.*

Table 3. Validated Host Software Tools – Release 8

SW Tools Name	Version
Mobile Broadband Package for Windows	MBPW_SDX65_R14.0.25_B5422
Mobile Broadband Package for Linux	MBPL_R43_0_25_B5402

3.1.4 Software Changes

Table 4. Software Changes – Release 8

ID	Item	Description	Impacted Domains
Protocol/Certification			
QTIX65-1879	IMEI SVN	Increased IMEI SVN to 11	PTCRB
QTIX65-1828	TS.25	Update hardcoded TS.25 list to 24-Feb-25	GSMA
RF			
QCT 3484732, 3365416	Disable VZW VoNR	Disable unsupported features (RAN network and core network readiness) from UE capability	RF
QTIX65-1847	BW improvement	3T NR CA combos can now support upto 300MHz (earlier limit was 200MHz)	RF
QTIX65-1766	Smart Transmit Improvement	Fixed rare crash observed in case of TDD bands with Smart Transmit enabled	RF
IMPULSE-2793	PC1.5, NR ULCA	Support added for 5G SA ULCA and support for PC1.5 on some of the TDD Bands *Refer to PTS update for more info*	RF
IMPULSE-173	2 Antenna Support	EM9291 can now support 2 Antenna configuration with reduced capabilities *Refer to upcoming Application Note for details*	RF

QTIX65-2087	Priority Smart Transmit	Improved ST to support, checking & using the rtsar_config_priority config file before the usual rtsar_config	RF
QTIX65-1891	Crash in B106	Fixed the known issue - crashing in B106 coverage in case module calibration does not include B106.	RF
QTIX65-2049	NR ULCA combos	Added non-tx switching NR ULCA combos	RF
QTIX65-1784	Combos addition	Added CS4.0, SA ULCA and PC1.5 combos from Qualcomm	RF
IMPULSE-3189	SA mode	Fixed issue - module stuck in SA mode	RF
Core			
QTIX65-1741	Module interaction with eSIM	NV's updated to ensure Host based LPA applications can always talk to eSIM	eSIM
QTIX65-1840	Merge MPSS.DE.4.0.c1-00452-OLYMPIC_GENALL_PACK-1.109079.2.114012.2	Security and stability improvements	SYSTEM
AT / QMI Commands			
QTIX65-1937	SUPL TLS1.2 support	AT!GPSTRANSSEC extended to support TLS 1.2 configuration option	SUPL
QTIX65-1922	QMI_NAS_SWI_GET_ANTENNA_SIG_INFO	Fixed conversion logic to report correct SINR value under QMI_NAS_SWI_GET_ANTENNA_SIG_INFO	RF
QTIX65-1915	AT!RFCID	Enabled AT!RFCID assignment at Lock Level 2 to select 2 Antenna solution.	2 Antenna Support
QTIX65-1904	AT!NRINFO	Fix pointer offset error in 2x2 MIMO AGC log packet parsing.	RF
QTIX65-1897	AT!SCUMMTU/QMI_SWI_DMS_SET_MTU	Upper limit updated to 9216bytes from 2000bytes for supporting Jumbo frames	DATA
QTIX65-1887	AT!UIMMAP	New command introduced to support eSIM profile download through UIM1 WWAN connection *For more details refer to AT Guide*	eSIM
QTIX65-1970	AT!STEFS	Smart Transmit AT command updates for v19/v20 compatibility solution	Smart Transmit
QTIX65-1925	AT!CELLLOCK	Added AT Command to lock module to EARFCN and PCI in LTE	RF
QTIX65-1971	AT!GPSEND	Fix AT port not working after GPSEND=0	GPS
QTIX65-1845	QMI_WDS_SWI_PROFILE_CHANGE indication	Added profile change indication when APN profiles are modified via carrier LWM2M	LWM2M
QTIX65-1831	AT!GPSTRANSSEC	Fixed at!gpstranssec to return Error in case of invalid input	GPS
Applications			

IMPULSE-2920	XLAT support for unique address	Configurable feature for obtaining unique IPv4 address with XLAT *Refer to upcoming revision of<CLAT App Note> for details*	XLAT
QTIX65-1863	Module enumeration on PCIe i/f with Windows Host	Due to Windows bug (under investigation) PCIe enumeration issue that happens in rare case is addressed by module change	PCIe
QTIX65-1934	GPS idle session	For END session, stopped sending locresultreport in IDLE state	GPS
QTIX65-1823	SMS default storage	SMS message is stored in "SM" by default, not in "ME"	SMS
QTIX65-1841	Antitheft SMS	Antitheft CONCAT SMS made invisible to other WMS clients	Antitheft
QTIX65-1842	Antitheft SMS	Added support for multi segment CONCAT SMS	Antitheft
QTIX65-1875	SIMPLA	Improve eSIM LPA customization handlers	eSIM
IMPULSE-3100	Large MTU support	Jumbo MTU is supported - Upper limit updated to 9216bytes	TCP/IP

3.1.5 Security Corrections/Improvements

As per EU/RED guidelines following change is done

1. L2 locked AT commands do not need any password coming out of Semtech Factory. Customers can still setup L2 password for their commercial deployment
2. Tcpdump package is removed which had significant number of vulnerabilities (CVE's). On need basis Semtech can provide a test build for this purpose

CVE	Description
CVE-2024-53014	Improper Validation of Array Index in Audio
CVE-2024-49838	Buffer Over-read in WLAN HOST
CVE-2024-53024	NULL Pointer Dereference in Display
CVE-2025-21430	Buffer Over-read in WLAN HOST
CVE-2024-53027	Buffer Copy Without Checking Size of Input ('Classic Buffer Overflow') in WLAN HOST
CVE-2025-21429	Buffer Over-read in WLAN HOST
CVE-2025-21424	Use After Free in NPU
CVE-2025-21450	Improper Authentication in GPS_GNSS
CVE-2025-21448	Buffer Over-read in WLAN Embedded SW
CVE-2025-21449	Buffer Over-read in WLAN Embedded SW
CVE-2025-21446	Buffer Over-read in WLAN Embedded SW

3.1.6 Known Issues

Note: *This section reflects known issues in Release 8 as of the Date of Generation UTC) indicated in the Release 8 Release Identification section above.*

Table 5. Known Issues – Release 8

ID	Issue	Description	Impacted Domains
Protocol/Certification			
RF			
QTIX65-2006	Not supported n40(tx)+n38/n41	n40(tx)+n38/n41 not supported due to hardware limitation - QPM6670 support DLCA 40R+41R only	RF
Core			
IMPULSE-2736	FOTA FW upgrade	FOTA failed when performing power cycle during installation	FOTA
IMPULSE-3154	Smart Transmit Compatibility	Due to stack revision from LE1.3 to LE1.3.1, existing v19 ST files may lead to crash in B106 coverage Issue addressed by new ST v20 generation mechanism for B106 SKU's	SMART TRANSMIT
AT / QMI Commands			

4 Firmware Release 7

Release 7 is released to support LTE B106 capable modules on new SKUs from the factory. The new SKUs are EM9291-1105284 and EM9293-1105285. Release-7 also adds a new Qualcomm Stack.

Release 7 firmware used on existing modules will crash when in B106 coverage (Refer to Known Issues 3.1.6 below)

For PRI details, see *[2] EM92xx PRI Customer Release Notes*.

4.1 Firmware Release Description

4.1.1 Firmware Release Identification

Table 6. Firmware Release Identification – Release 7

Component	Details
Firmware Version	SWIX65C_03.03.01.00
Date of generation (UTC)	2024/11/27 22:28:27
IMEI SV	10
GSMA TS.25	7-Oct-2024
Chipset Vendor Stack Version	MPSS.DE.4.0.c1-00427-OLYMPIC_GENALL_PACK-1.88272.3
Supported HW	EM9291, EM9293

4.1.2 Carrier Packages

Table 7. Carrier Packages – Release 7

Carrier	Firmware	Configuration	Comment
Approved			
ATT	SWIX65C_02.17.08.00	030.094_001	Release 6.1
BELL	SWIX65C_02.17.08.00	030.018_001	Release 6.1 - Accepted by Bell for Platform Certification
GENERIC	SWIX65C_02.17.08.00	030.081_001	Release 6.1
PTCRB	SWIX65C_02.17.08.00	030.077_001	Release 6.1
ROGERS	SWIX65C_02.17.08.00	030.033_001	Release 6.1
TMO	SWIX65C_02.17.08.00	030.042_001	Release 6.1
VERIZON	SWIX65C_02.17.08.00	030.092_001	Release 6.1
Approved Legacy			
ATT	SWIX65C_02.15.01.00	030.059_000	Release 2
BELL	SWIX65C_02.15.01.00	030.002_000	Release 2
GENERIC	SWIX65C_02.17.02.00	030.073_000	Release 5
GENERIC	SWIX65C_02.16.05.00	030.069_000	Release 4

GENERIC	SWIX65C_02.15.08.00	030.062_000	Release 3
GENERIC	SWIX65C_02.15.01.00	030.054_001	Release 2
GENERIC	SWIX65C_02.13.08.00	030.047_003	Release 1
PTCRB	SWIX65C_02.15.01.00	030.050_001	Release 2
PTCRB	SWIX65C_02.13.08.00	030.045_003	Release 1
TMO	SWIX65C_02.15.01.00	030.017_000	Release 2
VERIZON	SWIX65C_02.16.05.00	030.077_000	Release 4
VERIZON	SWIX65C_02.15.08.00	030.068_001	Release 3
Test			
ATT	SWIX65C_03.03.01.00	040.006_000	Release 7 BP4
BELL	SWIX65C_03.03.01.00	040.005_000	Release 7 BP4
DOCOMO	SWIX65C_03.03.01.00	040.006_000	Release 7 BP4
GENERIC	SWIX65C_03.03.01.00	040.007_000	Release 7 BP4
KDDI	SWIX65C_03.03.01.00	040.008_000	Release 7 BP4
PTCRB	SWIX65C_03.03.01.00	040.005_000	Release 7 BP4
ROGERS	SWIX65C_03.03.01.00	040.004_000	Release 7 BP4
SOFTBANK	SWIX65C_03.03.01.00	040.005_000	Release 7 BP4
TELSTRA	SWIX65C_03.03.01.00	040.005_000	Release 7 BP4
TELUS	SWIX65C_03.03.01.00	040.003_000	Release 7 BP4
TMO	SWIX65C_03.03.01.00	040.004_000	Release 7 BP4
VERIZON	SWIX65C_03.03.01.00	040.004_000	Release 7 BP4

4.1.3 Host Software Versions

The following tools were validated against this release.

Note: Semtech recommends upgrading to newer Host Software releases when available. Refer to applicable software release notes for any compatibility restrictions.

Table 8. Validated Host Software Tools – Release 7

SW Tools Name	Version
Mobile Broadband Package for Windows	MBPW_SDX65_R12.0.24_B5390
Mobile Broadband Package for Linux	MBPL_R42_0_24_B5388

4.1.4 Software Changes

Table 9. Software Changes – Release 7

ID	Item	Description	Impacted Domains
Protocol/Certification			
QTIX65-1732	IMEI SVN	Increased IMEI SVN to 10	PTCRB
QTIX65-1752	TS.25	Update hardcoded TS.25 list to 7-Oct-2024	GSMA
RF			
Core			
QTIX65-1761	Merge QTI stack LE1.3.1 r00442.1	- Improved Stability - For new modules, added support for B106, SA ULCA and PC1.5. - CR 3638204: - Fixed rare crash during throughput testing in ENDC	SYSTEM
QTIX65-1772	TCP Bi-directional Throughput	Some of the configuration settings are updated to improve TCP bi-directional throughput	DATA
IMPULSE-2807	SMS storage location	Fixed issue where SMS storage location is not consistent between AT and MBIM interfaces.	SMS
IMPULSE-2723	SMS Storage location	Fixed issue where SMS storage location is reset to "SM" after reset.	SMS
IMPULSE-2530	Rare crash after start-up	Fixed rare FW crash after startup.	STABILITY
AT / QMI Commands			
Applications			
IMPULSE-2334	AV FOTA Support	Support added for updating firmware on modules through Semtech AirVantage Server	AV FOTA
IMPULSE-810 QTIX65-1741	QMI_UIM_SEND_APDU	Removed restriction to allow host to use QMI_UIM_SEND_APDU as part of eSIM management	UIM
QTIX65-700	Smart Transmit QMI commands	Added QMI equivalents for QMI equivalent for AT!STEFS, AT!STPURSE and AT!STSTATUS	SMART TRANSMIT
IMPULSE-2652	Dying Gasp	Allow configuring Dying Gasp items when feature is disabled.	DYING GASP

QTIX65-1743	AT!GNSSCONFIG	Fixed options to enable/disable Galileo.	GNSS

4.1.5 Security Corrections/Improvements

CVE	Description
CVE-2024-45564	Use After Free in SPS-HLOS
CVE-2024-45544	Use After Free in Data HLOS - LNX
CVE-2024-45540	Use After Free in SPS-HLOS
CVE-2024-43057	Use After Free in MProc
CVE-2024-38426	when cache guard timer is running in LTE or NR, if network sends Authentication request with separation bit set in AMF, UE is not sending Authentication failure
CVE-2024-38423	Buffer Copy Without Checking Size of Input ('Classic Buffer Overflow') in Graphics_Linux
CVE-2024-38415	Use After Free in ComputerVision
CVE-2024-38414	Buffer Over-read in ComputerVision
CVE-2024-33071	Buffer Over-read in WLAN Host Cmn
CVE-2024-33070	Buffer Over-read in WLAN Host Cmn
CVE-2024-33068	Use After Free in WIN WLAN Host
CVE-2024-33064	Buffer Over-read in WLAN Host Cmn
CVE-2024-33060	Use After Free in DSP_Services
CVE-2024-33056	Buffer Over-read in MProc
CVE-2024-33051	Buffer Over-read in WLAN Embedded SW
CVE-2024-33045	Return of Stack Variable Address in Buses
CVE-2024-33037	Buffer Over-read in NPU
CVE-2024-33023	Use After Free in Graphics_Linux
CVE-2024-33016	Improper Restriction of Operations within the Bounds of a Memory Buffer in Storage
CVE-2024-33014	Buffer Over-read in WLAN Host Cmn
CVE-2024-33012	Buffer Over-read in WLAN Host Cmn
CVE-2024-33011	Buffer Over-read in WLAN Host Cmn
CVE-2024-33010	Use After Free in WLAN Host Cmn
CVE-2024-23376	Use After Free in ComputerVision
CVE-2024-23373	Use After Free in Graphics_Linux
CVE-2024-23368	Buffer Copy Without Checking Size of Input ('Classic Buffer Overflow') in MProc
CVE-2024-23364	Buffer Over-read in WLAN Embedded SW
CVE-2023-43552	Use After Free in WLAN Host Cmn
CVE-2023-43550	Integer Overflow or Wraparound in Services
CVE-2023-28587	Improper Restriction of Operations within the Bounds of a Memory Buffer in BTSOC

4.1.6 Known Issues

Note: This section reflects known issues in Release 5 as of the Date of Generation UTC) indicated in the Release 5 Release Identification section above.

Table 10. Known Issues – Release 7

ID	Issue	Description	Impacted Domains
Protocol/Certification			
Core			
IMPULSE-2876	B106 Compatibility	The Release-7 firmware will crash when used on modules with SKU numbers less than 1105284 AND the module sees/receives a B106 signal. The older modules do not have the necessary factory calibration for B106 to work. Customers are advised to use SKUs 1105284, 1105284 (or newer) for B106 testing	STABILITY
AT / QMI Commands			
Application			
IMPULSE-2735 IMPULSE-2736	AV FOTA Interruption	FOTA update through AV Server fails if there is power interruption during download/install use. Customer can restart FOTA to update modules successfully	AV FOTA

5 Firmware Release 6.2

Release 6.2 addresses an SMS issue and updates approved carrier packages.

For PRI details, see *[2] EM92xx PRI Customer Release Notes*.

5.1 Firmware Release Description

5.1.1 Firmware Release Identification

Table 11. Firmware Release Identification – Release 6.2

Component	Details
Firmware Version	SWIX65C_02.17.10.00
Date of generation (UTC)	2024/12/13 19:05:15
IMEI SV	6
GSMA TS.25	7-Oct-2024
Chipset Vendor Stack Version	MPSS.DE.3.0.c2-00197-OLYMPIC_GENALL_PACK-1.73325.4.74493.4
Supported HW	EM9291, EM9293

5.1.2 Carrier Packages

Table 12. Carrier Packages – Release 6.2

Carrier	Firmware	Configuration	Comment
Approved			
ATT	SWIX65C_02.17.08.00	030.094_001	Release 6.1
BELL	SWIX65C_02.17.08.00	030.018_001	Release 6.1 - Accepted by Bell for Platform Certification
DOCOMO	SWIX65C_02.17.08.00	030.023_002	Release 6.1
GENERIC	SWIX65C_02.17.10.00	030.086_000	Release 6.1
KDDI	SWIX65C_02.17.10.00	030.023_002	Release 6.2
PTCRB	SWIX65C_02.17.08.00	030.077_001	Release 6.1

ROGERS	SWIX65C_02.17.08.00	030.033_001	Release 6.1
SOFTBANK	SWIX65C_02.17.10.00	030.027_005	Release 6.2 – EM9291 Only
TELSTRA	SWIX65C_02.17.08.00	030.022_000	Release 6.1
TELUS	SWIX65C_02.17.08.00	030.028_002	Release 6.1
TMO	SWIX65C_02.17.08.00	030.042_001	Release 6.1
VERIZON	SWIX65C_02.17.08.00	030.092_001	Release 6.1
Approved Legacy			
ATT	SWIX65C_02.15.01.00	030.059_000	Release 2
BELL	SWIX65C_02.15.01.00	030.002_000	Release 2 - Accepted by Bell for Platform Certification
GENERIC	SWIX65C_02.17.08.00	030.081_001	Release 6.1
GENERIC	SWIX65C_02.17.02.00	030.073_000	Release 5
GENERIC	SWIX65C_02.16.05.00	030.069_000	Release 4
GENERIC	SWIX65C_02.15.08.00	030.062_000	Release 3
GENERIC	SWIX65C_02.15.01.00	030.054_001	Release 2
GENERIC	SWIX65C_02.13.08.00	030.047_003	Release 1
PTCRB	SWIX65C_02.15.01.00	030.050_001	Release 2
PTCRB	SWIX65C_02.13.08.00	030.045_003	Release 1
TMO	SWIX65C_02.15.01.00	030.017_000	Release 2
VERIZON	SWIX65C_02.16.05.00	030.077_000	Release 4
VERIZON	SWIX65C_02.15.08.00	030.068_001	Release 3
Test			
ATT	SWIX65C_02.17.10.00	030.098_000	Release 6.2
BELL	SWIX65C_02.17.10.00	030.022_000	Release 6.2
KDDI	SWIX65C_02.17.10.00	030.023_001	Release 6.2
PTCRB	SWIX65C_02.17.10.00	030.082_000	Release 6.2
ROGERS	SWIX65C_02.17.10.00	030.038_000	Release 6.2
TELSTRA	SWIX65C_02.17.10.00	030.027_000	Release 6.2
TELUS	SWIX65C_02.17.10.00	030.033_000	Release 6.2
TMO	SWIX65C_02.17.10.00	030.047_000	Release 6.2
VERIZON	SWIX65C_02.17.10.00	030.096_000	Release 6.2

5.1.3 Host Software Versions

The following tools were validated against this release.

Note: *Semtech recommends upgrading to newer Host Software releases when available. Refer to applicable software release notes for any compatibility restrictions.*

Table 13. Validated Host Software Tools – Release 6.2

SW Tools Name	Version
Mobile Broadband Package for Windows	MBPW_SDX65_R13.2.25_B5433
Mobile Broadband Package for Linux	M MBPL_R43_0_25_B5402

5.1.4 Software Changes

Table 14. Software Changes – Release 6.2

ID	Item	Description	Impacted Domains
Protocol/Certification			
QTIX65-1732	IMEI SVN	Increased IMEI SVN to 6	PTCRB
QTIX65-1752	TS.25	Update hardcoded TS.25 list to 7-Oct-2024	GSMA
IMPULSE-2908	Fixed KDDI IMS issue	Fixed issue with Re-REGISTER under MO barring cell	IMS
RF			
Core			
IMPULSE-2723	SMS storage location	Fixed issue where SMS storage location is reset to “SM” after reset.	SMS
IMPULSE-2807	SMS storage location	Fixed issue where SMS storage location is not consistent between AT and MBIM interfaces.	SMS
IMPULSE-2530	Rare crash after start-up	Fixed rare FW crash after startup.	STABILITY

AT / QMI Commands			
IMPULSE-810 QTIX65-1741	QMI_UIM_SEND_APDU	Removed restriction to allow host to use QMI_UIM_SEND_APDU	UIM
QTIX65-700	Smart Transmit QMI commands	Added QMI equivalents for QMI equivalent for AT!STEFS, AT!STPURSE and AT!STSTATUS	SMART TRANSMIT
IMPULSE-2652	Dying Gasp	Allow configuring Dying Gasp items when feature is disabled.	DYING GASP
QTIX65-1743	AT!GNSSCONFIG	Fixed options to enable/disable Galileo.	GNSS
QTIX65-1798	AT!GPSRF	Added support for displaying GPS RF information.	GNSS
IMPULSE-1189	Add QMI SAR commands	Add QMI commands equivalent to SAR AT commands	SAR
IMPULSE-504	AT!LTEINFO and QMI_NAS_SWI_GET_LTE_CA_CELL_INFO	Fixed SCC UL Bandwidth and UL MIMO layers reported in commands	RF
Applications			

5.1.5 Security Corrections/Improvements

No change from Release 6

5.1.6 Known Issues

Note: This section reflects known issues in Release 5 as of the Date of Generation UTC) indicated in the Release 5 Release Identification section above.

Table 15. Known Issues – Release 6.2

ID	Issue	Description	Impacted Domains
Protocol/Certification			
Core			
QTIX65-1766	Smart Transmit MTPL	Rare crash observed when using Smart Transmit	RF
AT / QMI Commands			

QTIX65-1897	AT!SCUMMTU and QMI_SWI_DMS_SET_MTU	AT!SCUMMTU and QMI_SWI_DMS_SET_MTU do not allow setting jumbo frames	

6 Firmware Release 6.1

Release 6.1 updates carrier packages.

For PRI details, see *[2] EM92xx PRI Customer Release Notes*.

6.1 Firmware Release Description

6.1.1 Firmware Release Identification

Table 16. Firmware Release Identification – Release 6

Component	Details
Firmware Version	SWIX65C_02.17.08.00
Date of generation (UTC)	2024/08/01 20:22:05
IMEI SV	5
GSMA TS.25	20-May-2024
Chipset Vendor Stack Version	MPSS.DE.3.0.c2-00197-OLYMPIC_GENALL_PACK-1.73325.4.74493.4
Supported HW	EM9291, EM9293

6.1.2 Carrier Packages

Table 17. Carrier Packages – Release 6.1

Carrier	Firmware	Configuration	Comment
Approved			
ATT	SWIX65C_02.17.08.00	030.094_001	Release 6.1
BELL	SWIX65C_02.17.08.00	030.018_001	Release 6.1
GENERIC	SWIX65C_02.17.08.00	030.081_001	Release 6.1
PTCRB	SWIX65C_02.17.08.00	030.077_001	Release 6.1
ROGERS	SWIX65C_02.17.08.00	030.033_001	Release 6.1
TMO	SWIX65C_02.17.08.00	030.042_001	Release 6.1
VERIZON	SWIX65C_02.17.08.00	030.092_001	Release 6.1
Approved Legacy			
ATT	SWIX65C_02.15.01.00	030.059_000	Release 2

BELL	SWIX65C_02.15.01.00	030.002_000	Release 2
GENERIC	SWIX65C_02.17.02.00	030.073_000	Release 5
GENERIC	SWIX65C_02.16.05.00	030.069_000	Release 4
GENERIC	SWIX65C_02.15.08.00	030.062_000	Release 3
GENERIC	SWIX65C_02.15.01.00	030.054_001	Release 2
GENERIC	SWIX65C_02.13.08.00	030.047_003	Release 1
PTCRB	SWIX65C_02.15.01.00	030.050_001	Release 2
PTCRB	SWIX65C_02.13.08.00	030.045_003	Release 1
TMO	SWIX65C_02.15.01.00	030.017_000	Release 2
VERIZON	SWIX65C_02.16.05.00	030.077_000	Release 4
VERIZON	SWIX65C_02.15.08.00	030.068_001	Release 3
Test			
DOCOMO	SWIX65C_02.17.08.00	030.023_001	Release 6.1
KDDI	SWIX65C_02.17.08.00	030.011_002	Release 6.1
SOFTBANK	SWIX65C_02.17.08.00	030.018_000	Release 6
TELSTRA	SWIX65C_02.17.08.00	030.022_000	Release 6
TELUS	SWIX65C_02.17.08.00	030.028_001	Release 6.1

6.1.3 Host Software Versions

The following tools were validated against this release.

Note: Semtech recommends upgrading to newer Host Software releases when available. Refer to applicable software release notes for any compatibility restrictions.

Table 18. Validated Host Software Tools – Release 6.1

SW Tools Name	Version
Mobile Broadband Package for Windows	MBPW_SDX65_R9.0.24_B5361
Mobile Broadband Package for Linux	MBPL_R39_0_24_B5364

6.1.4 Software Changes

No Changes from Release 6.

Table 19. Software Changes – Release 6.1

ID	Item	Description	Impacted Domains
Protocol/Certification			
RF			
Core			
AT / QMI Commands			
Applications			

6.1.5 Security Corrections/Improvements

No change from Release 6

6.1.6 Known Issues

Note: This section reflects known issues in Release 5 as of the Date of Generation UTC) indicated in the Release 5 Release Identification section above.

Table 20. Known Issues – Release 6.1

ID	Issue	Description	Impacted Domains
Protocol/Certification			
Core			
AT / QMI Commands			

7 Firmware Release 6

Release 6 addresses Bugs and Certification gating issues.

For PRI details, see *[2] EM92xx PRI Customer Release Notes*.

7.1 Firmware Release Description

7.1.1 Firmware Release Identification

Table 21. Firmware Release Identification – Release 6

Component	Details
Firmware Version	SWIX65C_02.17.08.00
Date of generation (UTC)	2024/08/01 20:22:05
IMEI SV	5
GSMA TS.25	20-May-2024
Chipset Vendor Stack Version	MPSS.DE.3.0.c2-00197-OLYMPIC_GENALL_PACK-1.73325.4.74493.4
Supported HW	EM9291, EM9293

7.1.2 Carrier Packages

Table 22. Carrier Packages – Release 6

Carrier	Firmware	Configuration	Comment
Approved			
ATT	SWIX65C_02.17.08.00	030.094_000	Release 6
BELL	SWIX65C_02.17.08.00	030.016_000	Release 6 - Accepted by Bell for Platform Certification
GCF (GENERIC)	SWIX65C_02.17.08.00	030.081_000	Release 6
PTCRB	SWIX65C_02.17.08.00	030.077_000	Release 6
TMO	SWIX65C_02.15.01.00	030.017_000	Release 2
VERIZON	SWIX65C_02.17.08.00	030.090_000	Release 6

Approved Legacy			
ATT	SWIX65C_02.15.01.00	030.059_000	Release 2
BELL	SWIX65C_02.15.01.00	030.002_000	Release 2 - Accepted by Bell for Platform Certification
GCF (GENERIC)	SWIX65C_02.17.02.00	030.073_000	Release 5
GCF (GENERIC)	SWIX65C_02.16.05.00	030.069_000	Release 4
GCF (GENERIC)	SWIX65C_02.15.08.00	030.062_000	Release 3
GCF (GENERIC)	SWIX65C_02.15.01.00	030.054_001	Release 2
GCF (GENERIC)	SWIX65C_02.13.08.00	030.047_003	Release 1
PTCRB	SWIX65C_02.15.01.00	030.050_001	Release 2
PTCRB	SWIX65C_02.13.08.00	030.045_003	Release 1
VERIZON	SWIX65C_02.16.05.00	030.077_000	Release 4
VERIZON	SWIX65C_02.15.08.00	030.068_001	Release 3
Test			
DISH	SWIX65C_02.17.08.00	030.027_000	Release 6
DOCOMO	SWIX65C_02.17.08.00	030.021_000	Release 6
KDDI	SWIX65C_02.17.08.00	030.011_000	Release 6
ROGERS	SWIX65C_02.17.08.00	030.033_000	Release 6
SOFTBANK	SWIX65C_02.17.08.00	030.014_000	Release 6
TELSTRA	SWIX65C_02.17.08.00	030.022_000	Release 6
TELUS	SWIX65C_02.17.08.00	030.028_000	Release 6
TMO	SWIX65C_02.17.08.00	030.042_000	Release 6

7.1.3 Host Software Versions

The following tools were validated against this release.

Note: Semtech recommends upgrading to newer Host Software releases when available. Refer to applicable software release notes for any compatibility restrictions.

Table 23. Validated Host Software Tools – Release 6

SW Tools Name	Version
Mobile Broadband Package for Windows	MBPW_SDX65_R9.0.24_B5361
Mobile Broadband Package for Linux	MBPL_R39_0_24_B5364

7.1.4 Software Changes

Table 24. Software Changes – Release 6

ID	Item	Description	Impacted Domains
Protocol/Certification			
QTIX65-1641	IMEI SVN	Increased IMEI SVN to 5	PTCRB
IMPULSE-2426 IMPULSE-2425 IMPULSE-2042 IMPULSE-2432	AT&T N14 SA test failures	Fixed issue where module was not registering on N14 SA	AT&T
CERTREQ-4357	Roaming PLMN not Registered	UE couldn't register after attach reject received with forbidden TAC – CR 3837235	AT&T
QTIX65-1650 IMPULSE-2255	IMS Registration	In rare cases, IMS registration fails after Firmware Update	IMS
SWIMDM-4605	TS.25	Update hardcoded TS.25 list to 20-May-2024	GSMA
RF			
QTIX65-1630 QTIX65-1628	Band Combination updates	Removed some LTE CA combos	RF
IMPULSE-2419	LTE ACL Failure in Mid bands at -30C	Fixed issue ACLR degradation in LTE at -30	RF
QTIX65-1623 IMPULSE-2573	MTPL Override Feature doesn't work in some corner-case scenarios	Fixed the scenarios where MCC changes after AT+CFUN=0/1	ST
QTIX65-1662 QTIX65-1695 IMPULSE-152	Antenna Tuner - GPIO	ANT_CTRL0 (Pin 59 on M.2) indicates Tx/Rx activity for B71/n71	Antenna
Core			
QTIX65-1502 IIMPULSE-2013	Firmware Upgrade stability testing	Fixed rare crash observed for WCDMA-RRC in MMOC component during internal stress testing	SYSTEM
QTIX65-1680 IMPULSE-2467	Firmware Version not returned on MBIM interface	MBIM_CID_DEVICE_CAPS handler updated to return FW version	MBIM
IMPULSE-2324	Rare crash observed with GNSS activities	Fixed rare crash when starting and stopping GNSS frequently.	GNSS
QTIX65-1668 IMPULSE-2273	Thermal Mitigation Level field removed from AT!GSTATUS output	Recommend using TMSTATUS to obtain TM Level for each TM Device	TM
QTIX65-1637 IMPULSE-1681	SIM Initialization issue on Android	Fix done to report QMI Object for SIM attribute in first SIM read attempt	SIM
QTIX65-1609 IMPULSE-2223	DTLS Auth Failures with one LWM2M server blocks Registration for other servers	Design improved to unblock Registration with other servers and continue retry with failed Server	LWM2M

QTIX65-1679 IMPULSE-1066	Wake Host function doesn't work for Device type configured as Embedded	Ignoring MBIM Shutdown event when SMS Wake feature is enabled for Embedded Device Type	WakeHost
AT / QMI Commands			
QTIX65-1612	AT!GSTATUS indicating stale RSSI values	RSSI for some of the Rx Path were stale which has now been fixed	RF
QTIX65-1549 IMPULSE-2138	AT!DARCONFIG updates	*mimo_mode* set to 1 now configures all 4 Receive paths instead of only MIMO1 and MIMO2	RF
QTIX65-1528	AT!RFSTINFO updates	To limit the size of output, additional arguments (Region, DSI) added to filter the results	RF
QTIX65-1669 IMPULSE-2320	5G NR Cell PCI not available under any AT Commands	New command AT!NRPCI? added for SA and NSA modes	RF
QTIX65-1505 IMPULSE-2113	Removed SDR1 and mmWave entries from TMSTATUS	SDR1 is only used for Rx and doesn't contribute to TM actions. mmWave is not supported on EM92	TM
QTIX65-1567 IMPULSE-1797	QMI_LOC_EVENT_GNSS_SV_INFO_IND	For system 3 (SBAS) invalid SVID was used	GNSS
QTIX65-1478	Remove AT!STIDX	This command is no used on EM92xx and therefore the support is removed	RF
Applications			
LE-16997	AirVantage revision	Fix revision string reported to AirVantage	AVC
LE-16998	Synchronization Failure	Remove unsupported service from EM92xx	AVC

7.1.5 Security Corrections/Improvements

No change from Release 5

7.1.6 Known Issues

Note: This section reflects known issues in Release 5 as of the Date of Generation UTC) indicated in the Release 5 Release Identification section above.

Table 25. Known Issues – Release 6

ID	Issue	Description	Impacted Domains
Protocol/Certification			

Core			
AT / QMI Commands			

8 Firmware Release 5

Release 5 addresses Bugs and brings in Security Improvements

For PRI details, see *[2] EM92xx PRI Customer Release Notes*.

8.1 Firmware Release Description

8.1.1 Firmware Release Identification

Table 26. Firmware Release Identification – Release 5

Component	Details
Firmware Version	SWIX65C_02.17.02.00
Date of generation (UTC)	2024/05/17 23:19:16
IMEI SV	4
GSMA TS.25	26-Feb-2024
Chipset Vendor Stack Version	MPSS.DE.3.0.c2-00197-OLYMPIC_GENALL_PACK-1.61239.4.69352.2
Supported HW	EM9291, EM9293

8.1.2 Carrier Packages

Table 27. Carrier Packages – Release 5

Carrier	Firmware	Configuration	Comment
Approved			
ATT	SWIX65C_02.15.01.00	030.059_000	Release 2
BELL	SWIX65C_02.15.01.00	030.002_000	Release 2 - Accepted by Bell for Platform Certification
GCF (GENERIC)	SWIX65C_02.17.02.00	030.073_000	Release 5
PTCRB	SWIX65C_02.15.01.00	030.050_001	Release 2
TMO	SWIX65C_02.15.01.00	030.017_000	Release 2
VERIZON	SWIX65C_02.16.05.00	030.077_000	Release 4
Approved Legacy			
GCF (GENERIC)	SWIX65C_02.16.05.00	030.069_000	Release 4

GCF (GENERIC)	SWIX65C_02.15.08.00	030.062_000	Release 3
GCF (GENERIC)	SWIX65C_02.15.01.00	030.054_001	Release 2
GCF (GENERIC)	SWIX65C_02.13.08.00	030.047_003	Release 1
PTCRB	SWIX65C_02.13.08.00	030.045_003	Release 1
VERIZON	SWIX65C_02.15.08.00	030.068_001	Release 3
Test			
ATT	SWIX65C_02.17.02.00	030.080_000	Release 5
BELL	SWIX65C_02.17.02.00	030.008_000	Release 5
DISH	SWIX65C_02.17.02.00	030.020_000	Release 5
DOCOMO	SWIX65C_02.17.02.00	030.013_000	Release 5
KDDI	SWIX65C_02.17.02.00	030.004_000	Release 5
PTCRB	SWIX65C_02.17.02.00	030.069_000	Release 5
ROGERS	SWIX65C_02.17.02.00	030.026_000	Release 5
SOFTBANK	SWIX65C_02.17.02.00	030.007_000	Release 5
TELSTRA	SWIX65C_02.17.02.00	030.010_000	Release 5
TELUS	SWIX65C_02.17.02.00	030.021_000	Release 5
TMO	SWIX65C_02.17.02.00	030.035_000	Release 5
VERIZON	SWIX65C_02.17.02.00	030.083_000	Release 5

8.1.3 Host Software Versions

The following tools were validated against this release.

Note: Semtech recommends upgrading to newer Host Software releases when available. Refer to applicable software release notes for any compatibility restrictions.

Table 28. Validated Host Software Tools – Release 5

SW Tools Name	Version
Mobile Broadband Package for Windows	MBPW_SDX65_R8.0.24_B5305
Mobile Broadband Package for Linux	MBPL_R39_0_24_B5364

8.1.4 Software Changes

Table 29. Software Changes – Release 5

ID	Item	Description	Impacted Domains
Protocol/Certification			
QTIX65-1621	IMEI SVN	Increased IMEI SVN to 4	PTCRB

RF			
IMPULSE-2344 QTIX65-1614	Smart Transmit MTPL	Address issues with Power Limits not being followed in the specific case of LTE ULCA with SCC on TDD	RF
Core			
QTIX65-1544	QTI stack update	Security and stability improvements	Core
AT / QMI Commands			
IMPULSE-2007 QTIX65-1506	AT!GPSCLRAASIST	Fixed issue where the AT command was not invalidating last valid location	GNSS
QTIX65-121	AT!GNSSCONFIG	NavIC can be enabled/disabled through additional parameter in GNSSCONFIG command	GNSS
QTIX65-1466	AT!GPSSUPLVER	Updated command to support 3-digit version	GNSS

8.1.5 Security Corrections/Improvements

Table 30. Security Corrections/Improvements – Release 5

CVE	Description
CVE-2023-33072	Buffer copy without checking size of Input ('Classic Buffer Overflow') in Core
CVE-2023-43556	Buffer Copy Without Checking Size of Input ('Classic Buffer Overflow') in Hypervisor
CVE-2024-21462	Buffer over-read in SCE-QTEE
CVE-2024-23362	Improper Input Validation in QWES
CVE-2024-23357	NULL Pointer Dereference in SPS-HLOS
CVE-2024-21461	Double Free in SPS_HLOS
CVE-2024-23356	Improper Restriction of Operations within the Bounds of a Memory Buffer in SPS-HLOS
CVE-2023-33087	Buffer Copy without Checking Size of Input (`Classic Buffer Overflow`) in MProc
CVE-2024-21475	Use of Out-of-range Pointer Offset in Video
CVE-2024-21467	Buffer Over-read in WLAN Host Cmn
CVE-2024-21480	Buffer Copy Without Checking Size of Input ('Classic Buffer Overflow') in Audio
CVE-2024-23371	Use After Free in Automotive Multimedia
CVE-2024-23374	Stack-based Buffer Overflow in PMIC
CVE-2024-23375	Buffer Copy Without Checking Size of Input ('Classic Buffer Overflow') in RIL
CVE-2024-33031	Improper Input Validation in RIL
CVE-2023-28578	Improper Input Validation in Services

8.1.6 Known Issues

Note: This section reflects known issues in Release 5 as of the Date of Generation UTC) indicated in the Release 5 Release Identification section above.

Table 31. Known Issues – Release 5

ID	Issue	Description	Impacted Domains
Protocol/Certification			
IMPULSE-1705	Unsupported 13289 v23.2 requirements	Limited support for newly added ENDC combos	AT&T
Core			
IMPULSE-152 IMPULSE-517	Antenna tuner - GPIO	ANTSEL0 (pin 59 on M.2 connector) is allocated for use, but not yet configurable with AT!ANTSEL	Antenna
AT / QMI Commands			

9 Firmware Release 4

Release 4 addresses issues with Verizon LWM2M which are required for Certification along with other Bug fixes For PRI details, see *[2] EM92xx PRI Customer Release Notes*.

9.1 Firmware Release Description

9.1.1 Firmware Release Identification

Table 32. Firmware Release Identification – Release 4

Component	Details
Firmware Version	SWIX65C_02.16.05.00
Date of generation (UTC)	2024/04/18 20:55:06
IMEI SV	3
GSMA TS.25	26-Feb-2024
Chipset Vendor Stack Version	MPSS.DE.3.0.c2-00171-OLYMPIC_GENALL_PACK-1.55632.5.61995.2
Supported HW	EM9291, EM9293

9.1.2 Carrier Packages

Table 33. Carrier Packages – Release 4

Carrier	Firmware	Configuration	Comment
Approved			
ATT	SWIX65C_02.15.01.00	030.059_000	Release 2
BELL	SWIX65C_02.15.01.00	030.002_000	Release 2 - Accepted by Bell for Platform Certification
GCF (GENERIC)	SWIX65C_02.16.05.00	030.069_000	Release 4
PTCRB	SWIX65C_02.15.01.00	030.050_001	Release 2
TMO	SWIX65C_02.15.01.00	030.017_000	Release 2
VERIZON	SWIX65C_02.16.05.00	030.077_000	Release 4
Approved Legacy			
GCF (GENERIC)	SWIX65C_02.15.08.00	030.062_000	Release 3

GCF (GENERIC)	SWIX65C_02.15.01.00	030.054_001	Release 2
GCF (GENERIC)	SWIX65C_02.13.08.00	030.047_003	Release 1
PTCRB	SWIX65C_02.13.08.00	030.045_003	Release 1
VERIZON	SWIX65C_02.15.08.00	030.068_001	Release 3
Test			
ATT	SWIX65C_02.16.05.00	030.074_000	Release 4
BELL	SWIX65C_02.16.05.00	030.003_000	Release 4
DISH	SWIX65C_02.16.05.00	030.015_000	Release 4
DOCOMO	SWIX65C_02.16.05.00	030.008_000	Release 4
PTCRB	SWIX65C_02.16.05.00	030.065_000	Release 4
ROGERS	SWIX65C_02.16.05.00	030.021_000	Release 4
SOFTBANK	SWIX65C_02.16.05.00	030.002_000	Release 4
TELSTRA	SWIX65C_02.16.05.00	030.006_000	Release 4
TELUS	SWIX65C_02.16.05.00	030.015_000	Release 4
TMO	SWIX65C_02.16.05.00	030.030_000	Release 4

9.1.3 Host Software Versions

The following tools were validated against this release.

Note: Semtech recommends upgrading to newer Host Software releases when available. Refer to applicable software release notes for any compatibility restrictions.

Table 34. Validated Host Software Tools – Release 4

SW Tools Name	Version
Mobile Broadband Package for Windows	MBPW_SDX65_R8.0.24_B5305
Mobile Broadband Package for Linux	MBPL_R38_0_24_B5347

9.1.4 Software Changes

Table 35. Software Changes – Release 4

ID	Item	Description	Impacted Domains
Protocol/Certification			
IMPULSE-2174 QTIX65-1587	Frequent Registration updated during Motive FOTA	Improvement by sending Registration Updated according to AET timer expiry requirement	Verizon LWM2M

IMPULSE-2106 QTIX65-1533	Disable Timeout for LWM2M server holding incorrect default value	Data Type corrected to store the right value	Verizon LWM2M
IMPULSE-769 QTIX65-1529	Unexpected Full Registration	Addressed issue where Module performs Full Registration when Lifetime timer has not expired.	Verizon LWM2M
IMPULSE-2074	DM commands timing out after successful Motive FOTA	IMS Registration failure after reboot has been fixed to address this issue	Verizon LWM2M
IMPULSE-1941 QTIX65-1575	Data Retry 2.6.7	Update default call settings to disable voice, CSD, and Emergency calls	Verizon Data Retry
SWIMDM-4427	TS.25	Updated to 26-Feb-2024	GSMA
RF			
IMPULSE-2325 QTIX65-1585	ARD impact on Thermal Mitigation	LTE and NR ARD is enabled by default to support one of the NR Thermal Mitigation policies.	RF / TM
IMPULSE-2259	AT!RXDEN	Fixed issue where AT command was not working for LTE and NR.	RF
IMPULSE-1509 QTIX65-1539	AT!RXDEN AT!NRINFO AT!GSTATUS	Fixed issue where AT command outputs may not be accurate in single-chain Rx mode	RF
IMPULSE-1995	AT!LTERXCONTROL	Fixed issue where AT command was not working for LTE CA	RF
IMPULSE-2297 QTIX65-1596	MTPL issue with SAR state change	Fixed issue where MTPL was not being applied on a SAR state change.	RF
IMPULSE-2032 IMPULSE-2046 IMPULSE-2033	Bandwidth allocation for band class B and above	Fixed bandwidth allocation for some combos with band class B and above.	RF
Core			
QTIX65-1515	Merge QTI stack r00476.1	Improved stability: - CR 3404908: fixed memory leak socket library. - CR 3343766: improved root certificate check on server.	SYSTEM
IMPULSE-2090 QTIX65-1541	Carrier Reset fails to clear persistence in some cases	Issue specific to carriers using Sub PRI (eg AT&T) is resolved now	IMSW
IMPULSE-2016 QTIX65-1599	Rare instances where Shutdown time is longer than expected	Fixes in shutdown function improving Shutdown time	SYSTEM
QTIX65-1559	IMS Registration fails for 5G SA mode	Fixed issue where IMS registration was not working for 5G SA	IMS
SWIMDM-4437	Subsystem Restart	Add initial support for SSR	Debug
SWIMDM-4401	Ramdump json	Escape special characters in ramdump json output	Debug
SWIMDM-4417	Ramdump reset	Allow ramdump tool to reset the module if in download mode	Debug
AT / QMI Commands			

SWIMDM-4472	Exhausted IPv6 PD	Fix return code for QMI_WDS_GET_DELEGATED_IPV6_PREFIX when all prefixes are exhausted	QMI
QTIX65-1585	AT!ARDEN	Added AT command to disable ARD to support lab testing.	AT
IMPULSE-2112 QTIX65-1589	AT!GSTATUS displays incorrect SCC channel value	Incorrect EARFCN limit removed for SCC Channels greater than 65535	AT

9.1.5 Security Corrections/Improvements

Table 36. Security Corrections/Improvements – Release 4

CVE	Description
CVE-2023-43542	Buffer Copy Without Checking Size of Input ('Classic Buffer Overflow') in QWES
CVE-2024-21469	Permissions, Privileges, and Access Control issues in SCE_QTEE
CVE-2024-21455	Untrusted Pointer Dereference in Audio
CVE-2024-21458	Buffer Over-read in WLAN HOST
CVE-2024-21471	Use After Free in Graphics_Linux
CVE-2023-33105	Configuration in WLAN Embedded SW
CVE-2024-23359	Buffer Over-read in MMCP
CVE-2024-21459	Buffer Over-read in WLAN HOST
CVE-2024-21463	Buffer Copy Without Checking Size of Input ('Classic Buffer Overflow') in Audio
CVE-2023-43522	NULL Pointer Dereference in WLAN Embedded SW
CVE-2023-43551	Improper Authentication in MMCP
CVE-2024-23354	Buffer Over-read in MMCP
CVE-2024-23353	Buffer Over-read in MMCP
CVE-2024-23352	Loop with Unreachable Exit Condition ('Infinite Loop') in MMCP

9.1.6 Known Issues

Note: This section reflects known issues in Release 4 as of the Date of Generation UTC) indicated in the Release 4 Release Identification section above.

Table 37. Known Issues – Release 4

ID	Issue	Description	Impacted Domains
Protocol/Certification			

IMPULSE-1703	Unsupported 13340 v23.2 requirements	Private network IMSI range 310-090 not supported	AT&T
IMPULSE-1705	Unsupported 13289 v23.2 requirements	Limited support for newly added ENDC combos	AT&T
Core			
IMPULSE-152 IMPULSE-517	Antenna tuner - GPIO	ANTSEL0 (pin 59 on M.2 connector) is allocated for use, but not yet configurable with AT!ANTSEL	Antenna
AT / QMI Commands			
QTIX65-121	NavIC	India NavIC GNSS constellation cannot be enabled/disabled by AT!GNSSCONFIG	GNSS

10 Firmware Release 3

Release 3 brings in critical bug fixes including fixes for future North American Certifications.

For PRI details, see *[2] EM92xx PRI Customer Release Notes*.

10.1 Firmware Release Description

10.1.1 Firmware Release Identification

Table 38. Firmware Release Identification – Release 3

Component	Details
Firmware Version	SWIX65C_02.15.08.00
Date of generation (UTC)	2023/11/17 22:12:47
IMEI SV	3
GSMA TS.25	20-Nov-2023
Chipset Vendor Stack Version	MPSS.DE.3.0.c2-00122-OLYMPIC_GENALL_PACK-1.52806.3.54036.2
Supported HW	EM9291, EM9293

10.1.2 Carrier Packages

Table 39. Carrier Packages – Release 3

Carrier	Firmware	Configuration	Comment
Approved			
ATT	SWIX65C_02.15.01.00	030.059_000	Release 2
GCF (GENERIC)	SWIX65C_02.15.08.00	030.062_000	Release 3
PTCRB	SWIX65C_02.15.01.00	030.050_001	Release 2
TMO	SWIX65C_02.15.01.00	030.017_000	Release 2
Approved Legacy			
GCF (GENERIC)	SWIX65C_02.15.01.00	030.054_001	Release 2
GCF (GENERIC)	SWIX65C_02.13.08.00	030.047_003	Release 1
PTCRB	SWIX65C_02.13.08.00	030.045_003	Release 1
Test			
ATT	SWIX65C_02.15.08.00	030.068_000	Release 3

BELL	SWIX65C_02.15.01.00	030.002_000	Release 2
DISH	SWIX65C_02.15.08.00	030.009_000	Release 3
DOCOMO	SWIX65C_02.15.08.00	030.002_000	Release 3
PTCRB	SWIX65C_02.15.08.00	030.058_000	Release 3
ROGERS	SWIX65C_02.15.08.00	030.015_000	Release 3
TELUS	SWIX65C_02.15.08.00	030.009_000	Release 3
TMO	SWIX65C_02.15.08.00	030.024_000	Release 3
VERIZON	SWIX65C_02.15.08.00	030.068_001	Release 3

10.1.3 Host Software Versions

The following tools were validated against this release.

Note: Semtech recommends upgrading to newer Host Software releases when available. Refer to applicable software release notes for any compatibility restrictions.

Table 40. Validated Host Software Tools – Release 3

SW Tools Name	Version
Mobile Broadband Package for Windows	MBPW_SDX65_R8.0.24_B5305
Mobile Broadband Package for Linux	MBPL_R38_0_24_B5347

10.1.4 Software Changes

Table 41. Software Changes – Release 3

ID	Item	Description	Impacted Domains
Protocol/Certification			
IMPULSE-1863 QTIX65-1503	OTA APN updates not observed in Windows	Windows ignores Class 3 APN update from module and pushes VZWINTERNET from its DB onto the module	Verizon GFIT
IMPULSE-765 QTIX65-1495	Intermittent FOTA failure	Issue is fixed by addressing memory leak in SSL component	Verizon LWM2M
IMPULSE-2096 QTIX65-1521	Module reporting “IoT Module” instead of “Module”	Verizon Requirement asks for module to report “Module” for LWM2M Object 3/0/17	Verizon LWM2M
IMPULSE-2106 QTIX65-1553	Unexpected value for node 1/3/5/ (Disable TO for Repo Server)	Issue addressed by correcting data type for storing node values	Verizon LWM2M

IMPULSE-2085 QTIX65-1523	Incorrect values reported for Default Min and Max for Repo server	For LWM2M Object 1/3/2 and 1/3/3 any value > 65535s is truncated storing incorrect value. Issue is fixed by proper type casting variables	Verizon LWM2M
QTIX65-1488	GID1-based APN	Add support for GID1-based APN switching	AT&T
SWIMDM-4324	TS.25	Updated to 20-Nov-2023	GSMA
QTIX65-1517	IMEI SVN	Increase IMEI SV to 3	PTCRB
RF			
QTIX65-1514	Smart Transmit MTPL	MTPL override feature can handle decimal values in Smart Transmit template.	RF
QTIX65-1481	Low Band power droop	Fix minor power droop across frequency on low band NR SA main/div antennas	RF
QTIX65-1414	AT!DARCONFIG	Update AT!DARCONFIG to not allow MIMO-only configuration downlink-only bands	AT
Core			
IMPULSE-1908 QTIX65-1503	Crash in Dlfe_fdpool_mgr.c	Fix rare modem crash during data transfer	Throughput
IMPULSE-1525 QTIX65-1407	Drop ICMP requests	Add support for module to silently drop incoming ICMP (ping) requests via ICMPINTSRVDIS customization	Data
SWIMDM-4385	Ramdump summary	Allow ramdump tool to capture json output with the -s parameter	Debugging
SWIMDM-4379	Ramdump startup status	Allow ramdump tool to capture the reboot reason in the json output	Debugging
IMPULSE-2013	Module in QDL mode after FW update	Fixed rare failure when upgrading from Release 1 to Release 2.	FW DL
AT / QMI Commands			

10.1.5 Security Corrections/Improvements

No change from Release 2.1.

10.1.6 Known Issues

Note: This section reflects known issues in Release 3 as of the Date of Generation UTC) indicated in the Release 3 Release Identification section above.

Table 42. Known Issues – Release 3

ID	Issue	Description	Impacted Domains
Protocol/Certification			
IMPULSE-1703	Unsupported 13340 v23.2 requirements	Private network IMSI range 310-090 not supported	AT&T
IMPULSE-1705	Unsupported 13289 v23.2 requirements	Limited support for newly added ENDC combos	AT&T
Various	Verizon LWM2M	General instability with LWM2M and FOTA	Verizon
Core			
IMPULSE-152 IMPULSE-517	Antenna tuner - GPIO	ANTSEL0 (pin 59 on M.2 connector) is allocated for use, but not yet configurable with AT!ANTSEL	Antenna
AT / QMI Commands			
SWIMDM-4331	Allow ?_? for firmware preference	Add support for '?' syntax in QMI_DMS_SET_FIRMWARE_PREF	QMI
IMPULSE-2112	AT!GSTATUS	Incorrect channel is displayed for LTE SCCs for channels greater than 65535.	AT
IMPULSE-2259	AT!RXDEN	AT command is not working for LTE	AT / RF
IMPULSE-1995	AT!LTERXCONTROL	AT command is not working for LTE	AT / RF

11 Firmware Release 2.1

Release 2.1 updates Release 2 with AT&T TA and updates Generic and PTCRB PRIs.

For PRI details, see *[2] EM92xx PRI Customer Release Notes*.

11.1 Firmware Release Description

11.1.1 Firmware Release Identification

Table 43. Firmware Release Identification – Release 2

Component	Details
Firmware Version	SWIX65C_02.15.01.00
Date of generation (UTC)	2023/11/17 22:12:47
IMEI SV	2
GSMA TS.25	25-Sep-2023
Chipset Vendor Stack Version	MPSS.DE.3.0.c2-00122-OLYMPIC_GENALL_PACK-1.49641.9
Supported HW	EM9291, EM9293

11.1.2 Carrier Packages

Table 44. Carrier Packages – Release 2

Carrier	Firmware	Configuration	Comment
Approved			
ATT	SWIX65C_02.15.01.00	030.059_000	Release 2
GCF (Generic)	SWIX65C_02.15.01.00	030.054_001	Release 2
PTCRB	SWIX65C_02.15.01.00	030.050_001	Release 2
TMO	SWIX65C_02.15.01.00	030.017_000	Release 2
Approved Legacy			
GCF (Generic)	SWIX65C_02.13.08.00	030.047_003	Release 1
PTCRB	SWIX65C_02.13.08.00	030.045_003	Release 1
Test			
ATT	SWIX65C_02.15.01.00	030.059_000	Release 2
DISH	SWIX65C_02.15.01.00	030.002_000	Release 2

ROGERS	SWIX65C_02.15.01.00	030.008_000	Release 2
TELUS	SWIX65C_02.15.01.00	030.002_001	Release 2
VERIZON	SWIX65C_02.15.01.00		

11.1.3 Host Software Versions

The following tools were validated against this release.

Note: Semtech recommends upgrading to newer Host Software releases when available. Refer to applicable software release notes for any compatibility restrictions.

Table 45. Validated Host Software Tools – Release 2.1

SW Tools Name	Version
Mobile Broadband Package for Windows	MBPW_SDX65_R7.0.23_B5304
Mobile Broadband Package for Linux	MBPL_R36_0_23_B5312

11.1.4 Software Changes

No change from Release

11.1.5 Security Corrections/Improvements

No change from Release 2.

11.1.6 Known Issues

Note: This section reflects known issues in Release 2 as of the Date of Generation UTC) indicated in the Release 2 Release Identification section above.

Table 46. Known Issues – Release 2

ID	Issue	Description	Impacted Domains
Protocol/Certification			
IMPULSE-765	Intermittent FOTA failure	Error during TLS handshake	Verizon

IMPULSE-1451	Unsupported 20261 v23.2 requirements	OTA APN test cases not supported: LTE-N90-9002 LTE-N91-9101 LTE-N91-9103	AT&T
IMPULSE-1703	Unsupported 13340 v23.2 requirements	Private network IMSI range 310-090 not supported	AT&T
IMPULSE-1705	Unsupported 13289 v23.2 requirements	Limited support for newly added ENDC combos	AT&T
IMPULSE-1863	OTA APN updates not observed in Windows	Use Windows COSA solution instead	APN
Core			
IMPULSE-152 IMPULSE-517	Antenna tuner - GPIO	ANTSEL0 (pin 59 on M.2 connector) is allocated for use, but not yet configurable with AT!ANTSEL	Antenna
IMPULSE-1908	Crash in Dlfe_fdpool_mgr.c	Rare modem cash during data transfer	Throughput
IMPULSE-2013	Module stuck in bootloader after FW update	Rare failure when upgrading from Release 1 leaves the module in the bootloader. The module does not enumerate in PCIe or USB. FW update is successful. To recover the module, a hard power cycle is required.	FW DL
QTIX65-1514	Smart Transmit MTPL for TDD bands	Maximum Transmit Power Level for TDD bands does not support decimal values in the Smart Transmit template.	RF
AT / QMI Commands			

12 Firmware Release 2

Release 2 adds support for North America carrier requirements, key features and critical bug fixes.

For PRI details, see *[2] EM92xx PRI Customer Release Notes*.

12.1 Firmware Release Description

12.1.1 Firmware Release Identification

Table 47. Firmware Release Identification – Release 2

Component	Details
Firmware Version	SWIX65C_02.15.01.00
Date of generation (UTC)	2023/11/17 22:12:47
IMEI SV	2
GSMA TS.25	25-Sep-2023
Chipset Vendor Stack Version	MPSS.DE.3.0.c2-00122-OLYMPIC_GENALL_PACK-1.49641.9
Supported HW	EM9291, EM9293

12.1.2 Carrier Packages

Table 48. Carrier Packages – Release 2

Carrier	Firmware	Configuration	Comment
Approved			
GCF	SWIX65C_02.15.01.00	030.054_001	Release 2
PTCRB	SWIX65C_02.13.08.00	030.045_003	Release 1
TMO	SWIX65C_02.15.01.00	030.017_000	Release 2
Approved Legacy			
GCF (Generic)	SWIX65C_02.13.08.00	030.047_003	Release 1
Test			
ATT	SWIX65C_02.15.01.00	030.059_000	Release 2
DISH	SWIX65C_02.15.01.00	030.002_000	Release 2
ROGERS	SWIX65C_02.15.01.00	030.008_000	Release 2
TELUS	SWIX65C_02.15.01.00	030.002_001	Release 2

VERIZON	SWIX65C_02.15.01.00	030.060_000	Release 2

12.1.3 Host Software Versions

The following tools were validated against this release.

Note: Semtech recommends upgrading to newer Host Software releases when available. Refer to applicable software release notes for any compatibility restrictions.

Table 49. Validated Host Software Tools – Release 2

SW Tools Name	Version
Mobile Broadband Package for Windows	MBPW_5G_B5273_R5.0.23
Mobile Broadband Package for Linux	MBPL_R35_B5311

12.1.4 Software Changes

Table 50. Software Changes – Release 2

ID	Item	Description	Impacted Domains
Protocol/Certification			
IMPULSE-1805	3GPP Release	Updated defaults to declare NR as 3GPP Release 16	3GPP
SWIMDM-4272	TS.25	Updated to 25-Sep-2023	GSMA
Core			
QTIX65-1454	QTI stack update	Security and stability improvements	Core
IMPULSE-73 IMPULSE-1535	Smart transmit	Initial feature support	RF
QTIX65-188	Boot redundancy	Add redundancy to bootloader as a recovery mechanism for a bootloader corruption scenario	Boot
QTIX65-1445	GNSS SUPL	Update SUPL settings to include 5G	GNSS
IMPULSE-1699	Windows 11 SV3	Fix connectivity issues reported by HLK	MBIM
IMPULSE-1520	Power consumption	Fix issue where idle power consumption was double the expected values in some scenarios	Power
IMPULSE-1592	XO Reliability	Improved tracking of XO drift across temperature	HW
IMPULSE-1803	FW download fails on Windows PCIe	MBPW R7 or newer drivers are required	FW DL

AT / QMI Commands			
QTIX65-1331	AT!SARSTATE	Add support for more than 20 states	AT
IMPULSE-1036	AT!RFCOMBOS	No longer return duplicate values	AT
IMPULSE-1658	AT!GSTATUS, AT!NRINFO	NR UL information is now displayed correctly	AT
IMPULSE-1675	AT!DATXCONTROL	Allow +26dBm max power for PC2	AT
QTIX65-1385	swiqmi_nas_get_nr5g_tx_power	Add NR Tx power	QMI

12.1.5 Security Corrections/Improvements

Table 51. Security Corrections/Improvements – Release 2

CVE	Description
CVE-2023-33080	Buffer over-read in WLAN Embedded SW
CVE-2022-33238	Loop with Unreachable Exit Condition (Infinite Loop) in WLAN Embedded SW
CVE-2022-40527	Reachable Assertion in WLAN Embedded SW
CVE-2023-33062	Buffer Over-read in WLAN Embedded SW
CVE-2023-33028	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') in WLAN Embedded SW
CVE-2023-33027	Buffer Over-read in WLAN Embedded SW
CVE-2023-33088	NULL pointer dereference in WLAN Embedded SW
CVE-2023-33089	NULL Pointer Dereference in WLAN Embedded SW
CVE-2023-33109	NULL Pointer Dereference in WLAN Embedded SW
CVE-2023-33098	Buffer Over-read in WLAN Embedded SW
CVE-2023-43511	Loop with Unreachable Exit Condition (Infinite Loop) in WLAN Embedded SW
CVE-2023-33047	Buffer Over-read in WLAN Embedded SW
CVE-2023-33076	Configuration Issue in Core
CVE-2023-33046	Time-of-check Time-of-use (TOCTOU) Race Condition in QWES
CVE-2023-33105	Does QCA fix WPA3 DoS Vulnerability ?
CVE-2023-33113	Buffer Copy Without Checking Size of Input ('Classic Buffer Overflow') in Kernel
CVE-2023-33106	Use of Out-of-range Pointer Offset in Graphics_Linux
CVE-2023-33072	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') in Core
CVE-2023-43521	Use After Free in SPS-HLOS
CVE-2023-33107	Integer Overflow or Wraparound in Graphics_Linux
CVE-2023-43542	Buffer Copy Without Checking Size of Input ('Classic Buffer Overflow') in QWES
CVE-2023-43513	Use of Out-of-range Pointer Offset in PCIe
CVE-2023-43536	Buffer Over-read in WLAN Embedded SW
CVE-2023-33112	Buffer Over-read in WLAN Embedded SW
CVE-2023-43533	Buffer Over-read in WLAN Embedded SW
CVE-2023-43544	Use After Free in Audio

CVE-2023-33103	Improper Input Validation in MMCP
CVE-2023-33104	Improper input Validation in MMCP
CVE-2023-33101	Incorrect typecasting Type Conversion or Cast in MMCP
CVE-2023-33100	Improper input validation in MMCP
CVE-2023-33099	Improper Input Validation in MMCP
CVE-2023-33086	Improper Release of Memory Before Removing Last Reference ('Memory Leak') in Data Modem
CVE-2023-33044	Reachable Assertion in Data Modem

12.1.6 Known Issues

Note: This section reflects known issues in Release 2 as of the Date of Generation UTC) indicated in the Release 2 Release Identification section above.

Table 52. Known Issues – Release 2

ID	Issue	Description	Impacted Domains
Protocol/Certification			
IMPULSE-765	Intermittent FOTA failure	Error during TLS handshake	Verizon
IMPULSE-1451	Unsupported 20261 v23.2 requirements	OTA APN test cases not supported: LTE-N90-9002 LTE-N91-9101 LTE-N91-9103	AT&T
IMPULSE-1703	Unsupported 13340 v23.2 requirements	Private network IMSI range 310-090 not supported	AT&T
IMPULSE-1705	Unsupported 13289 v23.2 requirements	Limited support for newly added ENDC combos	AT&T
IMPULSE-1863	OTA APN updates not observed in Windows	Use Windows COSA solution instead	APN
RF			
QTIX65-1514	Smart Transmit MTPL	MTPL override feature cannot handle decimal values in Smart Transmit template.	RF
Core			
IMPULSE-152 IMPULSE-517	Antenna tuner - GPIO	ANTSEL0 (pin 59 on M.2 connector) is allocated for use, but not yet configurable with AT!ANTSEL	Antenna
IMPULSE-1908	Crash in Dlfe_fdpool_mgr.c	Rare modem cash during data transfer	Throughput

IMPULSE-2013	Module stuck in bootloader after FW update	Rare failure when upgrading from Release 1 leaves the module in the bootloader. The module does not enumerate in PCIe or USB. FW update is successful. To recover the module, a hard power cycle is required.	FW DL
AT / QMI Commands			

13 Firmware Release 1

Release 1 is the first external commercial release, with PTCRB and GCF approval.

For PRI details, see *[2] EM92xx PRI Customer Release Notes*.

13.1 Firmware Release Description

13.1.1 Firmware Release Identification

Table 53. Firmware Release Identification – Release 1

Component	Details
Firmware Version	SWIX65C_02.13.08.00
Date of generation (UTC)	2023/09/20 16:15:21
IMEI SV	1
GSMA TS.25	14-Aug-2023
Chipset Vendor Stack Version	MPSS.DE.3.0.c2-00061-OLYMPIC_GENALL_PACK-1.40281.13.44579.3
Supported HW	EM9291, EM9293

13.1.2 Carrier Packages

Table 54. Carrier Packages – Release 1

Carrier	Firmware	Configuration	Comment
Approved			
GCF	SWIX65C_02.13.08.00	030.047_001	Release 1
PTCRB	SWIX65C_02.13.08.00	030.045_001	Release 1
Approved Legacy			
Test			
ATT	SWIX65C_02.13.08.00	030.052_000	Release 1
ROGERS	SWIX65C_02.13.08.00	030.003_000	Release 1
TMO	SWIX65C_02.13.08.00	030.012_000	Release 1
VERIZON	SWIX65C_02.13.08.00	030.053_000	Release 1

13.1.3 Host Software Versions

The following tools were validated against this release.

Note: *Semtech recommends upgrading to newer Host Software releases when available. Refer to applicable software release notes for any compatibility restrictions.*

Table 55. Validated Host Software Tools – Release #.#

SW Tools Name	Version
Mobile Broadband Package for Windows	MBPW_5G_B5273_R5.0.23
Mobile Broadband Package for Linux	MBPL_R35_B5311

13.1.4 Software Changes

Not applicable on first commercial release.

13.1.5 Security Corrections/Improvements

Not applicable on first commercial release.

13.1.6 Known Issues

Note: *This section reflects known issues in Release 1 as of the Date of Generation UTC) indicated in the Release 1 Release Identification section above.*

Table 56. Known Issues – Release 1

ID	Issue	Description	Impacted Domains
Protocol/Certification			
IMPULSE-1805	3GPP Release 16	Module is currently certified as a Release 15 device. This will be updated to Release 16 in the next release.	3GPP
Core			
IMPULSE-1520	Power consumption	Power consumption is higher than documented PTS values.	Power

IMPULSE-152 IMPULSE-517	Antenna tuner - GPIO	ANTSEL0 (pin 59 on M.2 connector) is allocated for use, but not yet configurable with AT!ANTSEL	Antenna
IMPULSE-73	Smart Transmit	Smart Transmit feature to be added in the next commercial release.	RF
AT / QMI Commands			
IMPULSE-1552	AT!DAUPDATEPARAM returns ERROR	This command is deprecated as it is no longer required. Customer Production Test Guide (41114569) and AT command guide (41113480) will be updated appropriately,	FTM
FW update			
IMPULSE-1802	FDT fails on PCIe	Windows FDT FW upgrade/downgrade often fails on PCIe. After failure a power cycle is required to recover the module. This also blocks host-based image switching. The issue is consistently reproduced on Win10 and intermittently on Win11. The issue is not observed over USB or Linux.	FDT
Host Connectivity			
IMPULSE-1699	Windows 11 SV3	Connections with Windows 11 SV3 (MBIM 4.0) will fail because Windows does not include the optional S-NSSAI TLV, and the module incorrectly expects it to be present.	Windows

14 Troubleshooting

14.1 QXDM Logging

To improve security, QXDM access is restricted by default.

To enable QXDM logging:

- Set AT!CUSTOM="DIAGENABLE",1. For additional information, see [3] EM9 Series AT Command Reference.

Please contact sierrawireless.com/support for any additional issues related to Sierra Wireless products.

15 Firmware Package Download Process

15.1 Windows Host via USB/PCIe

To download a firmware package on a Windows host:

1. Power on the EM9 module.
2. Make sure the latest driver is installed, and AT / DM ports over USB / PCIe are working from the host side.
3. Enter the following command:
   $ fdt2.exe -d g5k -f SWIX65C_02.13.08.00.cwe SWIX65C_02.13.08.00_GENERIC_030.047_000.nvu

15.2 Linux Host via USB / PCIe

To download a firmware package on a Linux host:

4. Power on the EM9 module
5. Make sure the latest driver is installed, the latest FW download tool is used, and AT / DM ports over USB / PCIe are working from the host side.
6. Copy SWIX65C_02.13.08.00_GENERIC_030.047_000.nvu to ./FW-PRI folder
7. Enter the following command:
   $ sudo ./fwdwl-litehostx86_64 -l mbim.log -f ../FW-PRI/ -t 1 -w SWIX65C_02.13.08.00.cwe SWIX65C_02.13.08.00_GENERIC_030.047_000.nvu

16 Related Documentation

Module resources, including product documentation, firmware packages and tools are published on The Source at https://source.sierrawireless.com.

Table 57. Reference Documents

Reference Document	Document #
[1] EM92 Migration Guide	41114768
[2] EM92xx PRI Customer Release Notes	41114792
[3] EM9 Series AT Command Reference	41113480
[4] EM929x Product Technical Specification	41114313

17 Abbreviations and Definitions

Table 58. Abbreviations and Acronyms

Abbreviation / Acronym	Definition
CVE	Common Vulnerabilities and Exposures
DV	Design Verification
FDT	Firmware Download Tool
FTM	Factory Test Mode
QMI	Qualcomm MSM Interface Qualcomm Modem Interface