Sierra Wireless WP76xx R17

Customer Release Notes

SIERRA WIRELESS®

41114724
Rev. 2

Important Notice

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

Safety and Hazards

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

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

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

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

Limitation of Liability

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

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

Copyright

Trademarks

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

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

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

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

Other trademarks are the property of their respective owners.

Contact Information

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

Revision History

Revision number	Release date	Changes
1.0	June 2023	Creation
2.0	July 2023	Updated timestamps for Modem Firmware in Release Identification

Contents

1: About this Document

This document describes WP76xx firmware releases.These release notes may be distributed to all direct and indirect customers.

1.1 Compatibility

1.1.1 Hardware Compatibility

Product Compatibility List
WP7605 – LTE Cat-4, LTE bands 1/3/8/11/18/19/21, WCDMA bands 1,6,19
WP7605-1 – LTE Cat-1, LTE bands 1/3/8/11/18/19/21, WCDMA bands 1,6,19
WP7607 - LTE Cat-4, LTE bands 1/3/7/8/20/28, WCDMA bands 1/8, GSM900/1800
WP7607-1 - LTE Cat-1, LTE bands 1/3/7/8/20/28, WCDMA bands 1/8, GSM900/1800
WP7608 - LTE Cat-4, LTE bands 1/3/5/8/40/41(partial) WCDMA bands 1/8, GSM900/1800
WP7608-1 - LTE Cat-1, LTE bands 1/3/5/8/40/41(partial) WCDMA bands 1/8, GSM900/1800
WP7609 - LTE Cat-4, LTE bands 1/3/5/7/8/28, WCDMA bands 1/5/8, GSM900/1800
WP7610 - LTE Cat-4, LTE bands 2/4/5/12/13/14/17/66, WCDMA bands 2/4/5
WP7611 – LTE Cat-4 LTE bands 2/4/5/12/13/14/25/26/66/71, WCDMA bands 2/4/5
WP7611-1 – LTE Cat-1, LTE bands 2/4/5/12/13/14/25/26/66/71, WCDMA bands 2/4/5

2: SWI9X07Y Release 17

Release 17 is a major milestone release with updates to Linux Kernel 4.14 and Yocto LTS 3.13, and crucial improvements for security vulnerabilities in WP7605, WP7607, WP7607-1, WP7608, WP7608-1, WP7609, WP7611, WP7611-1.

This release will be available to AirVantage IoT Cloud.

2.1 Software Release Description

Release 17 is the major FW release cadence, with Linux Kernel 4.14 and Yocto 3.1 LTS, and important improvements in security vulnerabilities for supported WP variants.

2.1.1 Release Identification

Component	Revision
Modem Firmware	SWI9X07Y_02.28.03.05 000000 jenkins 2019/07/08 11:04:16 (Telstra, DOCOMO, Softbank, KDDI) SWI9X07Y_02.32.03.01 000000 jenkins 2020/02/05 04:24:57 (LGU) SWI9X07Y_02.35.02.00 000000 jenkins 2019/11/07 01:30:36 (T-Mobile) SWI9X07Y_02.37.03.05 52ddef jenkins 2021/12/22 04:24:24 (AT&T) SWI9X07Y_02.37.06.05 b15b59 jenkins 2022/09/27 07:54:33 (Generic, Verizon)
Linux Firmware	SWI9X07Y_03.01.07.00 2023-03-16_13:18:36
MCU Firmware	002.015 (embedded as a binary in the Linux image, not applicable for modules without embedded MCU)
Legato Application Framework	21.05.2.rc2_7f59219499ecf02274c4ac7575e4f8c5
Binary Size	62.5 MB (compressed one-click Generic exe)
IMEI SV	6 (SWI9X07Y_02.28.03.05) 10 (SWI9X07Y_02.35.02.00) 13 (SWI9X07Y_02.32.03.01) 16 (SWI9X07Y_02.37.03.05) 18 (SWI9X07Y_02.37.06.05)
Qualcomm Stack Version	MDM9607.LE.2.0-00182-STD.PROD-1.264397.2
Linux Kernel Version	Linux version 4.14.253 (oe-user@oe-host) (gcc version 9.3.0 (GCC), GNU ld (GNU Binutils) 2.34.0.20200220) #1 PREEMPT Thu Mar 16 11:08:58 UTC 2023
Supported H/W	WP7605, WP7607, WP7607-1, WP7608, WP7608-1, WP7609, WP7611, WP7611-1

2.1.2 Software Tools Version

S/W Tools Name	Version
Windows Driver Package	B4956
Windows SDK	None
Skylight	None
Linux Drivers	S2.42N2.63
Linux SDK	SLQS04.00.26

Available in https://source.sierrawireless.com

2.1.3 Released Files

File	Carrier	Modem Firmware	Config	Linux Distribution	Base Legato System	Comment
WP7605 Approved Packages						
WP76xx_Release17_DOCOMO.exe	DOCOMO	SWI9X07Y_02.28.03.05	001.024_001	SWI9X07Y_03.01.07.00	21.05.2	DOCOMO Approved
WP76xx_Release17_SOFTBANK.exe	SoftBank	SWI9X07Y_02.28.03.05	001.028_001	SWI9X07Y_03.01.07.00	21.05.2	SoftBank Approved
WP76xx_Release17_KDDI.exe	KDDI	SWI9X07Y_02.28.03.05	001.026_002	SWI9X07Y_03.01.07.00	21.05.2	KDDI Approved
WP7607, WP7607-1 Approved Packages						
WP76xx_Release17_GENERIC.exe	GENERIC	SWI9X07Y_02.37.06.05	002.128_000	SWI9X07Y_03.01.07.00	21.05.2	GCF Approved
WP7608, WP7608-1 Approved Packages						
WP76xx_Release17_GENERIC.exe	GENERIC	SWI9X07Y_02.37.06.05	002.128_000	SWI9X07Y_03.01.07.00	21.05.2	GCF Approved
WP7609 Approved Packages						
WP76xx_Release17_TELSTRA.exe	TELSTRA	SWI9X07Y_02.28.03.05	001.058_001	SWI9X07Y_03.01.07.00	21.05.2	Telstra Approved
WP76xx_Release17_GENERIC.exe	GENERIC	SWI9X07Y_02.37.06.05	002.128_000	SWI9X07Y_03.01.07.00	21.05.2	GCF Approved
WP76xx_Release17_LGU.exe	LGU	SWI9X07Y_02.32.03.01	001.026_002	SWI9X07Y_03.01.07.00	21.05.2	LGU Approved
WP7611, WP7611-1 Approved Packages						
WP76xx_Release17_ATT.exe	ATT	SWI9X07Y_02.37.03.05	002.130_000	SWI9X07Y_03.01.07.00	21.05.2	AT&T Approved

WP76xx_Release17_GENERIC.exe	GENERIC	SWI9X07Y_02.37.06.05	002.128_000	SWI9X07Y_03.01.07.00	21.05.2	PTCRB Approved
WP76xx_Release17_VERIZON.exe	Verizon	SWI9X07Y_02.37.06.05	002.123_000	SWI9X07Y_03.01.07.00	21.05.2	Verizon Approved
WP76xx_Release17_TMO.exe	TMO	SWI9X07Y_02.35.02.00	001.017_001	SWI9X07Y_03.01.07.00	21.05.2	TMO Approved

Function	Files
Firmware components	9999999_9907152_SWI9X07Y_02.37.06.05_00_GENERIC_002.128_000.spk 9999999_9909268_SWI9X07Y_02.35.02.00_00_TMO_001.017_001.spk 9999999_9907255_SWI9X07Y_02.37.06.05_00_VERIZON_002.123_000.spk 9999999_9908843_SWI9X07Y_02.28.03.05_00_DOCOMO_001.024_001.spk 9999999_9909287_SWI9X07Y_02.32.03.01_00_LGU_001.026_002.spk 9999999_9907256_SWI9X07Y_02.37.03.05_00_ATT_002.130_000.spk 9999999_9908844_SWI9X07Y_02.28.03.05_00_SOFTBANK_001.028_001.spk 9999999_9908043_SWI9X07Y_02.28.03.05_00_TELSTRA_001.058_001.spk 9999999_9908845_SWI9X07Y_02.28.03.05_00_KDDI_001.026_002.spk linux-SWI9X07Y_03.01.07.00.cwe legato-21.05.2.rc2.cwe
Available in https://source.sierrawireless.com	

2.1.4 Available Memory Flash

Name	Partition	Allocation (kb)	Image Size (kb)	Usage
Linux Kernel	mtd12 (boot)	14336	9523	66%
Linux Rootfs	mtd13 (system)	60416	23552	38%
Legato Framework	mtd14 (lefwkro)	17664	6400	36%
SWIRW	mtd15 (swirw)	15872		
USERAPP	mtd16 (userapp)	133120		

2.1.4.1 RAM

RAM 57312 kB*

*Value is read from the MemAvailable parameter in /proc/meminfo after boot.

Note: Memory availability in Flash and RAM are for reference only and may vary depending on when it is measured and on the configurations made by the customer.

2.1.5 Boot Time

The following table lists the different service ready times since the first boot message.

The result was measured from WP7611-1 loaded with the Generic package. The boot time is for reference only and may vary depending on the configuration made by the customer.

Service ready	Time since first boot message	Description
Legato service ready	21 seconds	Legato framework and services have been fully initialized.
AT & QMI service ready	28 seconds	External host processor is now able to communicate with modules through AT commands (USB and UART) and/or QMI messages.
Legato application start	32 seconds	Customer Legato application starts running.

2.2 Software Changes Description

The following are changes in Release 17 since Release 16

Table 2-1: New Features

ID	Description
FORE-357	Yocto 3.1 LTS
FORE-256	Address Linux kernel threat surfaces
FORE-255	Linux Kernel Configuration Security Best Practices Recommendations
FORE-264	Linux Kernel 4.14
FORE-313	[8-wire UART] standard API ioctl() access to (DTR/DSR/DCD/RTS/RI
FORE-327	TrustZone 4.0 support
FORE-334	IOT Keystore
FORE-379	Anti-FW Rollback mechanism
FORE-375	Shared Key / AV Credentials Migration (Secure Storage to IOKS)

Table 2-2: Major Bug Fixes

ID	Description	Impacted Domain
QTI9X07-4953	[LwM2M][VZW] Store and resume observe requests over power cycle	Modem
QTI9X07-4956	[LwM2M][VZW] AET support	Modem
QTI9X07-5557	WP7611 failing Motive OOB FOTA	Modem

Table 2-2: Major Bug Fixes (Continued)

ID	Description	Impacted Domain
QTI9X07-4955	[LwM2M][VZW] Update Root CA certs	Modem
QTI9X07-5686	WP7611 LwM2M FOTA registration fail	Modem
QTI9X07-5688	Continuous handover between cells causes PS connection unstable when only main antenna (1RX) is configured - Single Rx mode.	Modem
QTI9X07-5693	Not enough number of observations (Expected Observations: 28 / Actual Observations: 1)	Modem
QTI9X07-5694	LwM2M fails with "Download Failed, error code 4"	Modem
QTI9X07-5701	Parse wrong hostname from DL-URL cause Motive FOTA download shows error code 4	Modem
QTI9X07-5702	LwM2M get net policy interface is wrong if have 2 clients use same PID	Modem
QTI9X07-5706	FOTA download restarts several times and eventually fails	Modem
QTI9X07-4928	[Legato] [Radio] le_mrc_AddPreferredOperator returns LE_UNSUPPORTED for available list of User Preferred operators in all networks	Legato
QTI9X07-4942	On Linux Android platform, while data call is active, USB connection disconnects momentarily with USB suspend/resume enabledUSB	USB
LE-16271 QTI9X07-5389 LE-16141	Add PRESENCE_EXTERNAL for SimMode.	Legato
LE-16195	Add API to get last CoAP error code of last push	Legato
LE-16199	Fix connection to AVC	Legato
LE-16149	Improvements to dataConnectionService in poor network conditions	Legato
LE-16157	Le_json max string size limit of 1 kB is too small for Octave	Legato
LE-16024	Do not attempt to free message on NULL return	Legato
LE-15906	Restore "Correct rpcProxy repack logic"	Legato
LE-15812	Optimize AT Proxy to re-use command buffer to store parameter list	Legato
ATSWI-173	Fixes FTP crash when too many sessions started	Legato
LE-15848	RPC memory corruption with wrong binding config	Legato
LE-15775	Module can not send/receive data to FTP server.	Legato
QTI9X07-5266	FOTA download cannot be resumed	Legato
LE-15819	Allow dynamic memory pool location	Legato
LE-15564	Improve cm data tool's input check and redundant back-to-back connects	Legato
LE-15549	Make RPC implementation of le_pack API out of line	Legato

Table 2-2: Major Bug Fixes (Continued)

ID	Description	Impacted Domain
LE-15538	Fix overflow if RPC num of bindings is not correct	Legato
LE-15500	Fix for FTP send causing AT port hang	Legato
LE-15082	Add session context support for LocalService	Legato
LE-13443 LE-13435 LE-13426	Fixed Legato RPC bugs	Legato
LE-14916	Add fa_thread_Pirority() to allow priority mapping	Legato
LE-15367	Let dcs_RemoveEventHandler always delete a client app's event handler upon process exit	Legato
LE-15336	Add missing libresolv.so.2 library	Legato
LE-15216	Fix buffer overflow error	Legato
LE-15409	Add UP event notification on an attempt to start a connection that results in LE_DUPLICATE	Legato
LE-14949	Fix cm data connect error	Legato
LE-15221	Fix possible memory leak in EventPool	Legato
LE-15177	Fix le_arg memory leak in handling positional argument	Legato
LE-14975	Support for asynchronous event handlers in RPC	Legato
LE-14992	Fix memory corruption in api_Messages pool	Legato
LE-15045	Add watchdogChain component requirement to missing components	Legato
LE-14596	Fix crash issues in AT+KHTTP commands	Legato
LE-14966	Location cannot sync with the AVMS server	Legato
LE-14691	Fix the crash caused by Network Reject Handler	Legato
LE-14705	Fix SecStore to enable recovery from corrupted key file	Legato
LE-14651	Stack size for threads in modemService are too large on Legato master	Legato
LE-13462	[sim] Automatically setting SIM PIN	Legato
LE-11198	Increase start session timeout	Legato
LE-13444 LE-13945	Integrate Qualcomm localhost fix	Legato
LE-14008 LE-14234	Follow HTTP/1.1 request standard	Legato
LE-14135	[fwupdate] Fix PA usage on Linux	Legato
LE-14065	Fix segFault in running Inspect on mutexes	Legato

Table 2-2: Major Bug Fixes (Continued)

ID	Description	Impacted Domain
LE-13724 LE-12711 LE-13674	Improve package downloader suspend / resume handling	Legato
LE-4096	Fix for FOTA being interrupted by sleep / ULPM	Legato
LE-13893	Add DNS server once cellular connection is established	Legato
LE-13838	Introduce SetPollingTimerInSeconds() for setting poll time in seconds than in minutes	Legato
LE-13758	Return stack sizes to 8K	Legato
LE-13748	[Start] Fix device stuck in sleep during rebooting	Legato
LE-13758	Increase stack size of all modemDaemon threads to 128K	Legato
	Increase modemService stack size to 128K	Legato
LE-16412	platformAdaptor/audio [Audio] Add NMMAP playback implementation	Audio
LE-16067	platformAdaptor/audio [AUDIO] Fix kernel issue with a work-around on audio playback in WP76xx	Audio
QTI9X07-5276	platformAdaptor/tzSwi—Kernel crashes when tz_GenerateKey is called using keysize = 0	tzSwi
LE-15788	platformAdaptor/tzSwi—Fix connecting to AVC when using IOTKeyStore	tzSwi
LE-15717	platformAdaptor/tzSwi—Fix memory leak in secStore app	tzSwi
LE-14705	platformAdaptor/tzSwi—Fix SecStore to enable recovery from corrupted key file	tzSwi
LE-15846	platformAdaptor/qmi—Fix sfs file handle leak	QMI
LE-14935	platformAdaptor/qmi—Add a mechanism to wait for QMI service start by other client	QMI
LE-14935	platformAdaptor/qmi—Module freezes on WDSS command after FW update with NV	QMI
LE-13289	platformAdaptor/qmi [FWUPDATE] Fix repeated reboot when swapping to a bad image	QMI
LE-12190	platformAdaptor/qmi—Lower PCI network scan timeout	QMI
LE-11939	platformAdaptor/qmi—Fix NVBACKUP fail	QMI
LE-13964	platformAdaptor/qmi—Adding DNS server based on session state	QMI
LE-13856 LE-13868	platformAdaptor/qmi—Cache profile data before data call	QMI
LE-13893	platformAdaptor/qmi—Add DNS server once cellular connection is established	QMI
LE-13880	platformAdaptor/qmi—Add profile handle initialization in some pa_mdc code	QMI

Table 2-2: Major Bug Fixes (Continued)

ID	Description	Impacted Domain
LE-13783 LE-13782	platformAdaptor/qmi—Add pa_mdc_qmi_profile.c for profile management using QMI	QMI
LE-13780	platformAdaptor/qmi—Implement get address functions	QMI
LE-10679	platformAdaptor/qmi [GNSS] Add trace log to GNSS to reduce the display of debug logs	QMI
LE-15683	Apps/AtQmiLinker—Add +ORP to hard-coded list of AT commands in atLinker.c	AtQmiLinker
LE-14046	Apps/AtQmiLinker—Handle illegal AT command syntax 'AT='	AtQmiLinker
LE-14049	Apps/AtQmiLinker—Enhance final response parsing logic	AtQmiLinker
LE-13915	Apps/AtQmiLinker—Enhance atFwdLinker response parsing logic	AtQmiLinker
LE-16803	Service/AirVantageConnector—Enable migration of secret BS every reboot / restore golden	AVC
LE-16430	Service/AirVantageConnector—Fix FOTA download unable to automatically resume in slow network	AVC
LE-16195	Service/AirVantageConnector—Add API to get last CoAP error code of last push	AVC
LE-15968	Service/AirVantageConnector—Fix SOTA suspend and resume download	AVC
LE-15716	Service/AirVantageConnector—Fix socket file descriptor leak	AVC
	Service/AirVantageConnector—Add adaption layer for socket closure	AVC
LE-15910	Service/AirVantageConnector—Fix FOTA blocked after upstream AVC from ulegato to Master	AVC
LE-15301 LE-15343	Service/AirVantageConnector—Fix SOTA suspend / resume issue	AVC
LE-14509	Service/AirVantageConnector—Fix fd closure process on server disconnect	AVC
LE-14115	Service/AirVantageConnector—Allow TPF download to be resumed	AVC
LE-14113	Service/AirVantageConnector—Introduce few optimizations to the code structure	AVC
LE-14114	Service/AirVantageConnector—Fix AVC Daemon crash when resuming a FOTA	AVC
LE-13724 LE-12711 LE-13674	Service/AirVantageConnectorÒImprove package downloader suspend / resume handling	AVC
LE-15965	Service/DataHub—Allow escape for all characters of a Json string	DataHub
LE-15180	Service/DataHub—Avoid killing client if adding a push handler fails	DataHub
LE-15238	Service/DataHub—Fix Datahub memory leak when pushing str samples	DataHub

Table 2-2: Major Bug Fixes (Continued)

ID	Description	Impacted Domain
HLLEAPP-775	external/github/gezedo/lwftp [HLLEAPP-775] Memory leak hangs module if FTP response is spread over multiple packets	lwftp
LE-13903	external/github/gezedo/lwftp [LE-13903] AT port is locked after sending kftprcv	lwftp
LE-13835	external/github/gezedo/lwftp [LE-13835] AT port is frozen after abort downloading an available file	lwftp

2.3 Security Corrections / Improvements

Table 2-3: CVE Fixes from Qualcomm

CVE-2004-1073	CVE-2005-0504	CVE-2005-2709	CVE-2005-3358	CVE-2006-0039
CVE-2006-0744	CVE-2006-1056	CVE-2006-1343	CVE-2006-1522	CVE-2006-1524
CVE-2006-1527	CVE-2006-1863	CVE-2006-1864	CVE-2006-2451	CVE-2006-3745
CVE-2006-4093	CVE-2006-4145	CVE-2006-5753	CVE-2006-6058	CVE-2007-2876
CVE-2007-3105	CVE-2007-4567	CVE-2007-4573	CVE-2008-1514	CVE-2008-3272
CVE-2008-3528	CVE-2008-3831	CVE-2008-5033	CVE-2008-5079	CVE-2009-0029
CVE-2009-0676	CVE-2009-0787	CVE-2009-2903	CVE-2009-3080	CVE-2009-4307
CVE-2009-4537	CVE-2009-4538	CVE-2010-1173	CVE-2010-1446	CVE-2010-2492
CVE-2010-2524	CVE-2010-2803	CVE-2010-2960	CVE-2010-2962	CVE-2010-3079
CVE-2010-3080	CVE-2010-3698	CVE-2010-3848	CVE-2010-3849	CVE-2010-3850
CVE-2010-4565	CVE-2011-0726	CVE-2011-1013	CVE-2011-1017	CVE-2011-1019
CVE-2011-1076	CVE-2011-1079	CVE-2011-1162	CVE-2011-2203	CVE-2011-2928
CVE-2011-3353	CVE-2012-0957	CVE-2012-1179	CVE-2012-2669	CVE-2012-3412
CVE-2012-3520	CVE-2012-4398	CVE-2012-4461	CVE-2012-4508	CVE-2013-0160
CVE-2013-0190	CVE-2013-0216	CVE-2013-0217	CVE-2013-0228	CVE-2013-0231
CVE-2013-0343	CVE-2013-0913	CVE-2013-1059	CVE-2013-1792	CVE-2013-1796
CVE-2013-1797	CVE-2013-1798	CVE-2013-2140	CVE-2013-2141	CVE-2013-2147
CVE-2013-2850	CVE-2013-2851	CVE-2013-2852	CVE-2013-2888	CVE-2013-2889
CVE-2013-2890	CVE-2013-2891	CVE-2013-2892	CVE-2013-2893	CVE-2013-2894
CVE-2013-2895	CVE-2013-2896	CVE-2013-2897	CVE-2013-2898	CVE-2013-2899
CVE-2013-2929	CVE-2013-2930	CVE-2013-4299	CVE-2013-4312	CVE-2013-4579
CVE-2013-4587	CVE-2013-6367	CVE-2013-6368	CVE-2013-6376	CVE-2014-0038
CVE-2014-0049	CVE-2014-0069	CVE-2014-0077	CVE-2014-0102	CVE-2014-0155

Table 2-3: CVE Fixes from Qualcomm (Continued)

CVE-2014-0181	CVE-2014-0196	CVE-2014-0206	CVE-2014-1739	CVE-2014-3153
CVE-2014-3534	CVE-2014-3601	CVE-2014-3610	CVE-2014-3611	CVE-2014-3631
CVE-2014-3646	CVE-2014-3647	CVE-2014-4014	CVE-2014-4171	CVE-2014-4508
CVE-2014-5207	CVE-2014-7970	CVE-2014-7975	CVE-2014-8134	CVE-2014-8159
CVE-2014-8480	CVE-2014-8481	CVE-2014-8989	CVE-2014-9529	CVE-2015-0239
CVE-2015-1333	CVE-2015-1350	CVE-2015-1593	CVE-2015-2150	CVE-2015-5157
CVE-2015-5257	CVE-2015-5307	CVE-2015-5327	CVE-2015-5697	CVE-2015-7513
CVE-2015-7550	CVE-2015-7799	CVE-2015-8104	CVE-2015-8543	CVE-2016-0728
CVE-2016-0758	CVE-2016-1583	CVE-2016-2085	CVE-2016-2117	CVE-2016-2143
CVE-2016-3136	CVE-2016-3137	CVE-2016-3713	CVE-2016-4440	CVE-2016-5400
CVE-2016-5412	CVE-2016-5828	CVE-2016-6162	CVE-2016-6213	CVE-2016-6480
CVE-2016-7039	CVE-2016-7042	CVE-2016-7097	CVE-2016-8399	CVE-2016-8405
CVE-2016-8630	CVE-2016-8650	CVE-2016-9191	CVE-2016-9604	CVE-2017-1000252
CVE-2017-1000365	CVE-2017-1000370	CVE-2017-11600	CVE-2017-12153	CVE-2017-12154
CVE-2017-12188	CVE-2017-12193	CVE-2017-15265	CVE-2017-16995	CVE-2017-16996
CVE-2017-17741	CVE-2017-2583	CVE-2017-2584	CVE-2017-2618	CVE-2017-2636
CVE-2017-5123	CVE-2017-6074	CVE-2017-6951	CVE-2017-7184	CVE-2017-7472
CVE-2017-7482	CVE-2017-7518	CVE-2017-7558	CVE-2017-7979	CVE-2017-8824
CVE-2018-1000004	CVE-2018-1000200	CVE-2018-10877	CVE-2018-10883	CVE-2018-1093
CVE-2018-14633	CVE-2018-9363	CVE-2019-11477	CVE-2019-11478	CVE-2019-11479
CVE-2019-14821	CVE-2019-14895	CVE-2019-14896	CVE-2019-19448	CVE-2019-3016
CVE-2019-3819	CVE-2019-3846	CVE-2019-3882	CVE-2020-12114	CVE-2020-14386
CVE-2020-24586	CVE-2020-24587	CVE-2020-24588	CVE-2020-25670	CVE-2020-25671
CVE-2020-26147	CVE-2021-22543	CVE-2021-3656		

Table 2-4: CVE Fixes from Sierra Linux Reference

CVE-1999-0061	CVE-1999-0074	CVE-1999-0128	CVE-1999-0138	CVE-1999-0165
CVE-1999-0171	CVE-1999-0183	CVE-1999-0195	CVE-1999-0216	CVE-1999-0245
CVE-1999-0257	CVE-1999-0317	CVE-1999-0330	CVE-1999-0381	CVE-1999-0400
CVE-1999-0401	CVE-1999-0414	CVE-1999-0431	CVE-1999-0451	CVE-1999-0460
CVE-1999-0461	CVE-1999-0513	CVE-1999-0590	CVE-1999-0628	CVE-1999-0720
CVE-1999-0780	CVE-1999-0781	CVE-1999-0782	CVE-1999-0804	CVE-1999-0986
CVE-1999-1018	CVE-1999-1166	CVE-1999-1225	CVE-1999-1276	CVE-1999-1285
CVE-1999-1339	CVE-1999-1341	CVE-1999-1352	CVE-1999-1441	CVE-1999-1442
CVE-2000-0006	CVE-2000-0227	CVE-2000-0289	CVE-2000-0344	CVE-2000-0506
CVE-2001-0316	CVE-2001-0317	CVE-2001-0405	CVE-2001-0851	CVE-2001-0907
CVE-2001-0914	CVE-2001-1056	CVE-2001-1244	CVE-2001-1273	CVE-2001-1384
CVE-2001-1390	CVE-2001-1391	CVE-2001-1392	CVE-2001-1393	CVE-2001-1394
CVE-2001-1395	CVE-2001-1396	CVE-2001-1397	CVE-2001-1398	CVE-2001-1399
CVE-2001-1400	CVE-2001-1551	CVE-2001-1572	CVE-2002-0046	CVE-2002-0060
CVE-2002-0429	CVE-2002-0499	CVE-2002-0510	CVE-2002-0570	CVE-2002-0704
CVE-2002-1319	CVE-2002-1380	CVE-2002-1571	CVE-2002-1572	CVE-2002-1573
CVE-2002-1574	CVE-2002-1963	CVE-2002-1976	CVE-2002-2254	CVE-2002-2438
CVE-2003-0001	CVE-2003-0018	CVE-2003-0127	CVE-2003-0187	CVE-2003-0244
CVE-2003-0246	CVE-2003-0418	CVE-2003-0462	CVE-2003-0465	CVE-2003-0467
CVE-2003-0476	CVE-2003-0501	CVE-2003-0619	CVE-2003-0643	CVE-2003-0956
CVE-2003-0961	CVE-2003-0984	CVE-2003-0985	CVE-2003-0986	CVE-2003-1040
CVE-2003-1161	CVE-2003-1604	CVE-2004-0001	CVE-2004-0003	CVE-2004-0010
CVE-2004-0058	CVE-2004-0075	CVE-2004-0077	CVE-2004-0109	CVE-2004-0133
CVE-2004-0138	CVE-2004-0177	CVE-2004-0178	CVE-2004-0181	CVE-2004-0186
CVE-2004-0228	CVE-2004-0229	CVE-2004-0394	CVE-2004-0415	CVE-2004-0424
CVE-2004-0427	CVE-2004-0447	CVE-2004-0495	CVE-2004-0496	CVE-2004-0497
CVE-2004-0535	CVE-2004-0554	CVE-2004-0565	CVE-2004-0596	CVE-2004-0626
CVE-2004-0658	CVE-2004-0685	CVE-2004-0812	CVE-2004-0814	CVE-2004-0816
CVE-2004-0883	CVE-2004-0887	CVE-2004-0949	CVE-2004-0986	CVE-2004-0997
CVE-2004-1016	CVE-2004-1017	CVE-2004-1056	CVE-2004-1057	CVE-2004-1058
CVE-2004-1068	CVE-2004-1069	CVE-2004-1070	CVE-2004-1071	CVE-2004-1072

Table 2-4: CVE Fixes from Sierra Linux Reference (Continued)

CVE-2004-1137	CVE-2004-1144	CVE-2004-1151	CVE-2004-1234	CVE-2004-1235
CVE-2004-1237	CVE-2004-1333	CVE-2004-1335	CVE-2004-2013	CVE-2004-2135
CVE-2004-2136	CVE-2004-2302	CVE-2004-2536	CVE-2004-2607	CVE-2004-2660
CVE-2004-2731	CVE-2005-0001	CVE-2005-0003	CVE-2005-0124	CVE-2005-0135
CVE-2005-0136	CVE-2005-0137	CVE-2005-0176	CVE-2005-0177	CVE-2005-0178
CVE-2005-0179	CVE-2005-0180	CVE-2005-0204	CVE-2005-0207	CVE-2005-0209
CVE-2005-0210	CVE-2005-0400	CVE-2005-0449	CVE-2005-0489	CVE-2005-0529
CVE-2005-0530	CVE-2005-0531	CVE-2005-0532	CVE-2005-0736	CVE-2005-0749
CVE-2005-0750	CVE-2005-0756	CVE-2005-0767	CVE-2005-0815	CVE-2005-0839
CVE-2005-0867	CVE-2005-0916	CVE-2005-0937	CVE-2005-0977	CVE-2005-1041
CVE-2005-1263	CVE-2005-1264	CVE-2005-1265	CVE-2005-1368	CVE-2005-1369
CVE-2005-1589	CVE-2005-1762	CVE-2005-1764	CVE-2005-1765	CVE-2005-1768
CVE-2005-1913	CVE-2005-2098	CVE-2005-2099	CVE-2005-2456	CVE-2005-2457
CVE-2005-2458	CVE-2005-2459	CVE-2005-2490	CVE-2005-2492	CVE-2005-2500
CVE-2005-2548	CVE-2005-2553	CVE-2005-2555	CVE-2005-2617	CVE-2005-2708
CVE-2005-2800	CVE-2005-2801	CVE-2005-2872	CVE-2005-2873	CVE-2005-2973
CVE-2005-3044	CVE-2005-3053	CVE-2005-3055	CVE-2005-3105	CVE-2005-3106
CVE-2005-3107	CVE-2005-3108	CVE-2005-3109	CVE-2005-3110	CVE-2005-3119
CVE-2005-3179	CVE-2005-3180	CVE-2005-3181	CVE-2005-3257	CVE-2005-3271
CVE-2005-3272	CVE-2005-3273	CVE-2005-3274	CVE-2005-3275	CVE-2005-3276
CVE-2005-3356	CVE-2005-3359	CVE-2005-3527	CVE-2005-3623	CVE-2005-3660
CVE-2005-3753	CVE-2005-3783	CVE-2005-3784	CVE-2005-3805	CVE-2005-3806
CVE-2005-3807	CVE-2005-3808	CVE-2005-3809	CVE-2005-3810	CVE-2005-3847
CVE-2005-3848	CVE-2005-3857	CVE-2005-3858	CVE-2005-4351	CVE-2005-4352
CVE-2005-4605	CVE-2005-4618	CVE-2005-4635	CVE-2005-4639	CVE-2005-4798
CVE-2005-4811	CVE-2005-4881	CVE-2005-4886	CVE-2006-0035	CVE-2006-0036
CVE-2006-0037	CVE-2006-0038	CVE-2006-0095	CVE-2006-0096	CVE-2006-0454
CVE-2006-0456	CVE-2006-0457	CVE-2006-0482	CVE-2006-0554	CVE-2006-0555
CVE-2006-0557	CVE-2006-0558	CVE-2006-0741	CVE-2006-0742	CVE-2006-1052
CVE-2006-1055	CVE-2006-1066	CVE-2006-1242	CVE-2006-1342	CVE-2006-1368
CVE-2006-1523	CVE-2006-1525	CVE-2006-1528	CVE-2006-1624	CVE-2006-1855
CVE-2006-1856	CVE-2006-1857	CVE-2006-1858	CVE-2006-1859	CVE-2006-1860

Table 2-4: CVE Fixes from Sierra Linux Reference (Continued)

CVE-2006-1862	CVE-2006-2071	CVE-2006-2444	CVE-2006-2445	CVE-2006-2446
CVE-2006-2448	CVE-2006-2629	CVE-2006-2934	CVE-2006-2935	CVE-2006-2936
CVE-2006-3085	CVE-2006-3468	CVE-2006-3626	CVE-2006-3634	CVE-2006-3635
CVE-2006-3741	CVE-2006-4535	CVE-2006-4538	CVE-2006-4572	CVE-2006-4623
CVE-2006-4663	CVE-2006-4813	CVE-2006-4814	CVE-2006-4997	CVE-2006-5158
CVE-2006-5173	CVE-2006-5174	CVE-2006-5331	CVE-2006-5619	CVE-2006-5701
CVE-2006-5749	CVE-2006-5751	CVE-2006-5754	CVE-2006-5755	CVE-2006-5757
CVE-2006-5823	CVE-2006-5871	CVE-2006-6053	CVE-2006-6054	CVE-2006-6056
CVE-2006-6057	CVE-2006-6060	CVE-2006-6106	CVE-2006-6128	CVE-2006-6304
CVE-2006-6333	CVE-2006-6535	CVE-2006-6921	CVE-2006-7051	CVE-2006-7203
CVE-2006-7229	CVE-2007-0006	CVE-2007-0771	CVE-2007-0772	CVE-2007-0822
CVE-2007-0958	CVE-2007-0997	CVE-2007-1000	CVE-2007-1217	CVE-2007-1353
CVE-2007-1357	CVE-2007-1388	CVE-2007-1496	CVE-2007-1497	CVE-2007-1592
CVE-2007-1730	CVE-2007-1734	CVE-2007-1861	CVE-2007-2172	CVE-2007-2451
CVE-2007-2453	CVE-2007-2480	CVE-2007-2525	CVE-2007-2875	CVE-2007-2878
CVE-2007-3104	CVE-2007-3107	CVE-2007-3380	CVE-2007-3513	CVE-2007-3642
CVE-2007-3719	CVE-2007-3720	CVE-2007-3731	CVE-2007-3732	CVE-2007-3740
CVE-2007-3843	CVE-2007-3848	CVE-2007-3850	CVE-2007-3851	CVE-2007-4133
CVE-2007-4311	CVE-2007-4571	CVE-2007-4774	CVE-2007-4997	CVE-2007-5087
CVE-2007-5093	CVE-2007-5498	CVE-2007-5500	CVE-2007-5501	CVE-2007-5904
CVE-2007-5966	CVE-2007-6063	CVE-2007-6151	CVE-2007-6206	CVE-2007-6417
CVE-2007-6434	CVE-2007-6694	CVE-2007-6712	CVE-2007-6716	CVE-2007-6733
CVE-2007-6761	CVE-2007-6762	CVE-2008-0001	CVE-2008-0007	CVE-2008-0009
CVE-2008-0010	CVE-2008-0163	CVE-2008-0352	CVE-2008-0598	CVE-2008-0600
CVE-2008-1294	CVE-2008-1375	CVE-2008-1669	CVE-2008-1673	CVE-2008-1675
CVE-2008-2136	CVE-2008-2137	CVE-2008-2148	CVE-2008-2358	CVE-2008-2365
CVE-2008-2372	CVE-2008-2729	CVE-2008-2750	CVE-2008-2812	CVE-2008-2826
CVE-2008-2931	CVE-2008-2944	CVE-2008-3077	CVE-2008-3247	CVE-2008-3275
CVE-2008-3276	CVE-2008-3496	CVE-2008-3525	CVE-2008-3526	CVE-2008-3527
CVE-2008-3534	CVE-2008-3535	CVE-2008-3686	CVE-2008-3792	CVE-2008-3833
CVE-2008-3911	CVE-2008-3915	CVE-2008-4113	CVE-2008-4210	CVE-2008-4302
CVE-2008-4307	CVE-2008-4395	CVE-2008-4410	CVE-2008-4445	CVE-2008-4554

Table 2-4: CVE Fixes from Sierra Linux Reference (Continued)

CVE-2008-4576	CVE-2008-4618	CVE-2008-4933	CVE-2008-4934	CVE-2008-5025
CVE-2008-5029	CVE-2008-5134	CVE-2008-5182	CVE-2008-5300	CVE-2008-5395
CVE-2008-5700	CVE-2008-5701	CVE-2008-5702	CVE-2008-5713	CVE-2008-6107
CVE-2008-7256	CVE-2008-7316	CVE-2009-0024	CVE-2009-0028	CVE-2009-0031
CVE-2009-0065	CVE-2009-0269	CVE-2009-0322	CVE-2009-0605	CVE-2009-0675
CVE-2009-0745	CVE-2009-0746	CVE-2009-0747	CVE-2009-0748	CVE-2009-0778
CVE-2009-0834	CVE-2009-0835	CVE-2009-0859	CVE-2009-0935	CVE-2009-1046
CVE-2009-1072	CVE-2009-1184	CVE-2009-1192	CVE-2009-1242	CVE-2009-1243
CVE-2009-1265	CVE-2009-1298	CVE-2009-1336	CVE-2009-1337	CVE-2009-1338
CVE-2009-1360	CVE-2009-1385	CVE-2009-1388	CVE-2009-1389	CVE-2009-1439
CVE-2009-1527	CVE-2009-1630	CVE-2009-1633	CVE-2009-1883	CVE-2009-1895
CVE-2009-1897	CVE-2009-1914	CVE-2009-1961	CVE-2009-2287	CVE-2009-2406
CVE-2009-2407	CVE-2009-2584	CVE-2009-2691	CVE-2009-2692	CVE-2009-2695
CVE-2009-2698	CVE-2009-2767	CVE-2009-2768	CVE-2009-2844	CVE-2009-2846
CVE-2009-2847	CVE-2009-2848	CVE-2009-2849	CVE-2009-2908	CVE-2009-2909
CVE-2009-2910	CVE-2009-3001	CVE-2009-3002	CVE-2009-3043	CVE-2009-3228
CVE-2009-3234	CVE-2009-3238	CVE-2009-3280	CVE-2009-3286	CVE-2009-3288
CVE-2009-3290	CVE-2009-3547	CVE-2009-3556	CVE-2009-3612	CVE-2009-3613
CVE-2009-3620	CVE-2009-3621	CVE-2009-3623	CVE-2009-3624	CVE-2009-3638
CVE-2009-3640	CVE-2009-3722	CVE-2009-3725	CVE-2009-3726	CVE-2009-3888
CVE-2009-3889	CVE-2009-3939	CVE-2009-4004	CVE-2009-4005	CVE-2009-4020
CVE-2009-4021	CVE-2009-4026	CVE-2009-4027	CVE-2009-4031	CVE-2009-4067
CVE-2009-4131	CVE-2009-4138	CVE-2009-4141	CVE-2009-4271	CVE-2009-4272
CVE-2009-4306	CVE-2009-4308	CVE-2009-4410	CVE-2009-4536	CVE-2009-4895
CVE-2010-0003	CVE-2010-0006	CVE-2010-0007	CVE-2010-0008	CVE-2010-0291
CVE-2010-0307	CVE-2010-0410	CVE-2010-0415	CVE-2010-0437	CVE-2010-0622
CVE-2010-0623	CVE-2010-0727	CVE-2010-0741	CVE-2010-1083	CVE-2010-1084
CVE-2010-1085	CVE-2010-1086	CVE-2010-1087	CVE-2010-1088	CVE-2010-1146
CVE-2010-1148	CVE-2010-1162	CVE-2010-1187	CVE-2010-1188	CVE-2010-1436
CVE-2010-1437	CVE-2010-1451	CVE-2010-1488	CVE-2010-1636	CVE-2010-1641
CVE-2010-1643	CVE-2010-2066	CVE-2010-2071	CVE-2010-2226	CVE-2010-2240
CVE-2010-2243	CVE-2010-2248	CVE-2010-2478	CVE-2010-2495	CVE-2010-2521

Table 2-4: CVE Fixes from Sierra Linux Reference (Continued)

CVE-2010-2525	CVE-2010-2537	CVE-2010-2538	CVE-2010-2653	CVE-2010-2798
CVE-2010-2938	CVE-2010-2942	CVE-2010-2943	CVE-2010-2946	CVE-2010-2954
CVE-2010-2955	CVE-2010-2959	CVE-2010-2963	CVE-2010-3015	CVE-2010-3066
CVE-2010-3067	CVE-2010-3078	CVE-2010-3081	CVE-2010-3084	CVE-2010-3086
CVE-2010-3296	CVE-2010-3297	CVE-2010-3298	CVE-2010-3301	CVE-2010-3310
CVE-2010-3432	CVE-2010-3437	CVE-2010-3442	CVE-2010-3448	CVE-2010-3477
CVE-2010-3705	CVE-2010-3858	CVE-2010-3859	CVE-2010-3861	CVE-2010-3865
CVE-2010-3873	CVE-2010-3874	CVE-2010-3875	CVE-2010-3876	CVE-2010-3877
CVE-2010-3880	CVE-2010-3881	CVE-2010-3904	CVE-2010-4072	CVE-2010-4073
CVE-2010-4074	CVE-2010-4075	CVE-2010-4076	CVE-2010-4077	CVE-2010-4078
CVE-2010-4079	CVE-2010-4080	CVE-2010-4081	CVE-2010-4082	CVE-2010-4083
CVE-2010-4157	CVE-2010-4158	CVE-2010-4160	CVE-2010-4161	CVE-2010-4162
CVE-2010-4163	CVE-2010-4164	CVE-2010-4165	CVE-2010-4169	CVE-2010-4175
CVE-2010-4242	CVE-2010-4243	CVE-2010-4248	CVE-2010-4249	CVE-2010-4250
CVE-2010-4251	CVE-2010-4256	CVE-2010-4258	CVE-2010-4263	CVE-2010-4342
CVE-2010-4343	CVE-2010-4346	CVE-2010-4347	CVE-2010-4525	CVE-2010-4526
CVE-2010-4527	CVE-2010-4529	CVE-2010-4648	CVE-2010-4649	CVE-2010-4650
CVE-2010-4655	CVE-2010-4656	CVE-2010-4668	CVE-2010-4805	CVE-2010-5313
CVE-2010-5328	CVE-2010-5329	CVE-2010-5331	CVE-2010-5332	CVE-2011-0006
CVE-2011-0463	CVE-2011-0521	CVE-2011-0695	CVE-2011-0699	CVE-2011-0709
CVE-2011-0710	CVE-2011-0711	CVE-2011-0712	CVE-2011-0714	CVE-2011-0716
CVE-2011-0999	CVE-2011-1010	CVE-2011-1012	CVE-2011-1016	CVE-2011-1020
CVE-2011-1021	CVE-2011-1023	CVE-2011-1044	CVE-2011-1078	CVE-2011-1080
CVE-2011-1082	CVE-2011-1083	CVE-2011-1090	CVE-2011-1093	CVE-2011-1160
CVE-2011-1163	CVE-2011-1169	CVE-2011-1170	CVE-2011-1171	CVE-2011-1172
CVE-2011-1173	CVE-2011-1180	CVE-2011-1182	CVE-2011-1474	CVE-2011-1476
CVE-2011-1477	CVE-2011-1478	CVE-2011-1479	CVE-2011-1493	CVE-2011-1494
CVE-2011-1495	CVE-2011-1573	CVE-2011-1576	CVE-2011-1577	CVE-2011-1581
CVE-2011-1585	CVE-2011-1593	CVE-2011-1598	CVE-2011-1745	CVE-2011-1746
CVE-2011-1747	CVE-2011-1748	CVE-2011-1759	CVE-2011-1767	CVE-2011-1768
CVE-2011-1770	CVE-2011-1771	CVE-2011-1776	CVE-2011-1833	CVE-2011-1927
CVE-2011-2022	CVE-2011-2182	CVE-2011-2183	CVE-2011-2184	CVE-2011-2189

Table 2-4: CVE Fixes from Sierra Linux Reference (Continued)

CVE-2011-2208	CVE-2011-2209	CVE-2011-2210	CVE-2011-2211	CVE-2011-2213
CVE-2011-2479	CVE-2011-2482	CVE-2011-2484	CVE-2011-2491	CVE-2011-2492
CVE-2011-2493	CVE-2011-2494	CVE-2011-2495	CVE-2011-2496	CVE-2011-2497
CVE-2011-2498	CVE-2011-2517	CVE-2011-2518	CVE-2011-2521	CVE-2011-2525
CVE-2011-2534	CVE-2011-2689	CVE-2011-2695	CVE-2011-2699	CVE-2011-2700
CVE-2011-2707	CVE-2011-2723	CVE-2011-2898	CVE-2011-2905	CVE-2011-2906
CVE-2011-2909	CVE-2011-2918	CVE-2011-2942	CVE-2011-3188	CVE-2011-3191
CVE-2011-3209	CVE-2011-3359	CVE-2011-3363	CVE-2011-3593	CVE-2011-3619
CVE-2011-3637	CVE-2011-3638	CVE-2011-4077	CVE-2011-4080	CVE-2011-4081
CVE-2011-4086	CVE-2011-4087	CVE-2011-4097	CVE-2011-4098	CVE-2011-4110
CVE-2011-4112	CVE-2011-4127	CVE-2011-4131	CVE-2011-4132	CVE-2011-4324
CVE-2011-4325	CVE-2011-4326	CVE-2011-4330	CVE-2011-4347	CVE-2011-4348
CVE-2011-4594	CVE-2011-4604	CVE-2011-4611	CVE-2011-4621	CVE-2011-4913
CVE-2011-4914	CVE-2011-4915	CVE-2011-4916	CVE-2011-4917	CVE-2011-5321
CVE-2011-5327	CVE-2012-0028	CVE-2012-0038	CVE-2012-0044	CVE-2012-0045
CVE-2012-0055	CVE-2012-0056	CVE-2012-0058	CVE-2012-0207	CVE-2012-0810
CVE-2012-0879	CVE-2012-1090	CVE-2012-1097	CVE-2012-1146	CVE-2012-1583
CVE-2012-1601	CVE-2012-2100	CVE-2012-2119	CVE-2012-2121	CVE-2012-2123
CVE-2012-2127	CVE-2012-2133	CVE-2012-2136	CVE-2012-2137	CVE-2012-2313
CVE-2012-2319	CVE-2012-2372	CVE-2012-2373	CVE-2012-2375	CVE-2012-2383
CVE-2012-2384	CVE-2012-2390	CVE-2012-2744	CVE-2012-2745	CVE-2012-3364
CVE-2012-3375	CVE-2012-3400	CVE-2012-3430	CVE-2012-3510	CVE-2012-3511
CVE-2012-3552	CVE-2012-4444	CVE-2012-4467	CVE-2012-4530	CVE-2012-4542
CVE-2012-4565	CVE-2012-5374	CVE-2012-5375	CVE-2012-5517	CVE-2012-5532
CVE-2012-6536	CVE-2012-6537	CVE-2012-6538	CVE-2012-6539	CVE-2012-6540
CVE-2012-6541	CVE-2012-6542	CVE-2012-6543	CVE-2012-6544	CVE-2012-6545
CVE-2012-6546	CVE-2012-6547	CVE-2012-6548	CVE-2012-6549	CVE-2012-6638
CVE-2012-6647	CVE-2012-6657	CVE-2012-6689	CVE-2012-6701	CVE-2012-6703
CVE-2012-6704	CVE-2012-6712	CVE-2013-0268	CVE-2013-0290	CVE-2013-0309
CVE-2013-0310	CVE-2013-0311	CVE-2013-0313	CVE-2013-0349	CVE-2013-0871
CVE-2013-0914	CVE-2013-1763	CVE-2013-1767	CVE-2013-1772	CVE-2013-1773
CVE-2013-1774	CVE-2013-1819	CVE-2013-1826	CVE-2013-1827	CVE-2013-1828

Table 2-4: CVE Fixes from Sierra Linux Reference (Continued)

CVE-2013-1848	CVE-2013-1858	CVE-2013-1860	CVE-2013-1928	CVE-2013-1929
CVE-2013-1943	CVE-2013-1956	CVE-2013-1957	CVE-2013-1958	CVE-2013-1959
CVE-2013-1979	CVE-2013-2015	CVE-2013-2017	CVE-2013-2058	CVE-2013-2094
CVE-2013-2128	CVE-2013-2146	CVE-2013-2148	CVE-2013-2164	CVE-2013-2206
CVE-2013-2232	CVE-2013-2234	CVE-2013-2237	CVE-2013-2546	CVE-2013-2547
CVE-2013-2548	CVE-2013-2596	CVE-2013-2634	CVE-2013-2635	CVE-2013-2636
CVE-2013-3076	CVE-2013-3222	CVE-2013-3223	CVE-2013-3224	CVE-2013-3225
CVE-2013-3226	CVE-2013-3227	CVE-2013-3228	CVE-2013-3229	CVE-2013-3230
CVE-2013-3231	CVE-2013-3232	CVE-2013-3233	CVE-2013-3234	CVE-2013-3235
CVE-2013-3236	CVE-2013-3237	CVE-2013-3301	CVE-2013-3302	CVE-2013-4125
CVE-2013-4127	CVE-2013-4129	CVE-2013-4162	CVE-2013-4163	CVE-2013-4205
CVE-2013-4220	CVE-2013-4247	CVE-2013-4254	CVE-2013-4270	CVE-2013-4300
CVE-2013-4343	CVE-2013-4345	CVE-2013-4348	CVE-2013-4350	CVE-2013-4387
CVE-2013-4470	CVE-2013-4483	CVE-2013-4511	CVE-2013-4512	CVE-2013-4513
CVE-2013-4514	CVE-2013-4515	CVE-2013-4516	CVE-2013-4563	CVE-2013-4588
CVE-2013-4591	CVE-2013-4592	CVE-2013-5634	CVE-2013-6282	CVE-2013-6378
CVE-2013-6380	CVE-2013-6381	CVE-2013-6382	CVE-2013-6383	CVE-2013-6431
CVE-2013-6432	CVE-2013-6763	CVE-2013-7026	CVE-2013-7027	CVE-2013-7263
CVE-2013-7264	CVE-2013-7265	CVE-2013-7266	CVE-2013-7267	CVE-2013-7268
CVE-2013-7269	CVE-2013-7270	CVE-2013-7271	CVE-2013-7281	CVE-2013-7339
CVE-2013-7348	CVE-2013-7421	CVE-2013-7445	CVE-2013-7446	CVE-2013-7470
CVE-2014-0100	CVE-2014-0101	CVE-2014-0131	CVE-2014-0203	CVE-2014-0205
CVE-2014-1438	CVE-2014-1444	CVE-2014-1445	CVE-2014-1446	CVE-2014-1690
CVE-2014-1737	CVE-2014-1738	CVE-2014-1874	CVE-2014-2038	CVE-2014-2039
CVE-2014-2309	CVE-2014-2523	CVE-2014-2568	CVE-2014-2672	CVE-2014-2673
CVE-2014-2678	CVE-2014-2706	CVE-2014-2739	CVE-2014-2851	CVE-2014-2889
CVE-2014-3122	CVE-2014-3144	CVE-2014-3145	CVE-2014-3180	CVE-2014-3181
CVE-2014-3182	CVE-2014-3183	CVE-2014-3184	CVE-2014-3185	CVE-2014-3186
CVE-2014-3535	CVE-2014-3645	CVE-2014-3673	CVE-2014-3687	CVE-2014-3688
CVE-2014-3690	CVE-2014-3917	CVE-2014-3940	CVE-2014-4027	CVE-2014-4157
CVE-2014-4322	CVE-2014-4323	CVE-2014-4608	CVE-2014-4611	CVE-2014-4652
CVE-2014-4653	CVE-2014-4654	CVE-2014-4655	CVE-2014-4656	CVE-2014-4667

Table 2-4: CVE Fixes from Sierra Linux Reference (Continued)

CVE-2014-4699	CVE-2014-4943	CVE-2014-5045	CVE-2014-5077	CVE-2014-5206
CVE-2014-5332	CVE-2014-5471	CVE-2014-5472	CVE-2014-6410	CVE-2014-6416
CVE-2014-6417	CVE-2014-6418	CVE-2014-7145	CVE-2014-7207	CVE-2014-7283
CVE-2014-7284	CVE-2014-7822	CVE-2014-7825	CVE-2014-7826	CVE-2014-7841
CVE-2014-7842	CVE-2014-7843	CVE-2014-8086	CVE-2014-8133	CVE-2014-8160
CVE-2014-8172	CVE-2014-8173	CVE-2014-8369	CVE-2014-8559	CVE-2014-8709
CVE-2014-8884	CVE-2014-9090	CVE-2014-9322	CVE-2014-9410	CVE-2014-9419
CVE-2014-9420	CVE-2014-9428	CVE-2014-9584	CVE-2014-9585	CVE-2014-9644
CVE-2014-9683	CVE-2014-9710	CVE-2014-9715	CVE-2014-9717	CVE-2014-9728
CVE-2014-9729	CVE-2014-9730	CVE-2014-9731	CVE-2014-9803	CVE-2014-9870
CVE-2014-9888	CVE-2014-9892	CVE-2014-9895	CVE-2014-9900	CVE-2014-9903
CVE-2014-9904	CVE-2014-9914	CVE-2014-9922	CVE-2014-9940	CVE-2015-0274
CVE-2015-0275	CVE-2015-0568	CVE-2015-0572	CVE-2015-0573	CVE-2015-1328
CVE-2015-1339	CVE-2015-1420	CVE-2015-1421	CVE-2015-1465	CVE-2015-1573
CVE-2015-1805	CVE-2015-2041	CVE-2015-2042	CVE-2015-2666	CVE-2015-2672
CVE-2015-2686	CVE-2015-2830	CVE-2015-2922	CVE-2015-2925	CVE-2015-3212
CVE-2015-3214	CVE-2015-3288	CVE-2015-3290	CVE-2015-3291	CVE-2015-3331
CVE-2015-3332	CVE-2015-3339	CVE-2015-3636	CVE-2015-4001	CVE-2015-4002
CVE-2015-4003	CVE-2015-4004	CVE-2015-4036	CVE-2015-4167	CVE-2015-4170
CVE-2015-4176	CVE-2015-4177	CVE-2015-4178	CVE-2015-4692	CVE-2015-4700
CVE-2015-5156	CVE-2015-5283	CVE-2015-5364	CVE-2015-5366	CVE-2015-5706
CVE-2015-5707	CVE-2015-6252	CVE-2015-6526	CVE-2015-6937	CVE-2015-7509
CVE-2015-7515	CVE-2015-7566	CVE-2015-7613	CVE-2015-7872	CVE-2015-7884
CVE-2015-7885	CVE-2015-7990	CVE-2015-8019	CVE-2015-8215	CVE-2015-8324
CVE-2015-8374	CVE-2015-8539	CVE-2015-8551	CVE-2015-8569	CVE-2015-8575
CVE-2015-8660	CVE-2015-8709	CVE-2015-8746	CVE-2015-8767	CVE-2015-8785
CVE-2015-8787	CVE-2015-8812	CVE-2015-8816	CVE-2015-8830	CVE-2015-8839
CVE-2015-8844	CVE-2015-8845	CVE-2015-8944	CVE-2015-8950	CVE-2015-8952
CVE-2015-8953	CVE-2015-8955	CVE-2015-8956	CVE-2015-8961	CVE-2015-8962
CVE-2015-8963	CVE-2015-8964	CVE-2015-8966	CVE-2015-8967	CVE-2015-8970
CVE-2015-9004	CVE-2015-9289	CVE-2016-0723	CVE-2016-0821	CVE-2016-0823
CVE-2016-10044	CVE-2016-10088	CVE-2016-10147	CVE-2016-10150	CVE-2016-10153

Table 2-4: CVE Fixes from Sierra Linux Reference (Continued)

CVE-2016-10154	CVE-2016-10200	CVE-2016-10208	CVE-2016-10229	CVE-2016-10277
CVE-2016-10283	CVE-2016-10284	CVE-2016-10285	CVE-2016-10286	CVE-2016-10287
CVE-2016-10288	CVE-2016-10289	CVE-2016-10290	CVE-2016-10291	CVE-2016-10292
CVE-2016-10293	CVE-2016-10294	CVE-2016-10295	CVE-2016-10296	CVE-2016-10318
CVE-2016-10741	CVE-2016-10764	CVE-2016-10905	CVE-2016-10906	CVE-2016-10907
CVE-2016-1237	CVE-2016-1575	CVE-2016-1576	CVE-2016-2053	CVE-2016-2059
CVE-2016-2061	CVE-2016-2062	CVE-2016-2063	CVE-2016-2064	CVE-2016-2065
CVE-2016-2066	CVE-2016-2067	CVE-2016-2068	CVE-2016-2069	CVE-2016-2070
CVE-2016-2184	CVE-2016-2185	CVE-2016-2186	CVE-2016-2187	CVE-2016-2188
CVE-2016-2383	CVE-2016-2384	CVE-2016-2543	CVE-2016-2544	CVE-2016-2545
CVE-2016-2546	CVE-2016-2547	CVE-2016-2548	CVE-2016-2549	CVE-2016-2550
CVE-2016-2782	CVE-2016-2847	CVE-2016-3070	CVE-2016-3134	CVE-2016-3135
CVE-2016-3138	CVE-2016-3139	CVE-2016-3140	CVE-2016-3156	CVE-2016-3672
CVE-2016-3689	CVE-2016-3841	CVE-2016-3951	CVE-2016-3955	CVE-2016-4470
CVE-2016-4482	CVE-2016-4485	CVE-2016-4486	CVE-2016-4557	CVE-2016-4558
CVE-2016-4565	CVE-2016-4568	CVE-2016-4569	CVE-2016-4578	CVE-2016-4580
CVE-2016-4581	CVE-2016-4794	CVE-2016-4805	CVE-2016-4913	CVE-2016-4951
CVE-2016-4997	CVE-2016-4998	CVE-2016-5195	CVE-2016-5243	CVE-2016-5244
CVE-2016-5340	CVE-2016-5342	CVE-2016-5343	CVE-2016-5344	CVE-2016-5696
CVE-2016-5728	CVE-2016-5829	CVE-2016-5856	CVE-2016-5870	CVE-2016-6130
CVE-2016-6136	CVE-2016-6156	CVE-2016-6187	CVE-2016-6197	CVE-2016-6198
CVE-2016-6327	CVE-2016-6516	CVE-2016-6755	CVE-2016-6756	CVE-2016-6757
CVE-2016-6758	CVE-2016-6759	CVE-2016-6760	CVE-2016-6761	CVE-2016-6775
CVE-2016-6776	CVE-2016-6777	CVE-2016-6778	CVE-2016-6779	CVE-2016-6780
CVE-2016-6781	CVE-2016-6782	CVE-2016-6785	CVE-2016-6786	CVE-2016-6787
CVE-2016-6789	CVE-2016-6790	CVE-2016-6791	CVE-2016-6828	CVE-2016-7117
CVE-2016-7425	CVE-2016-7910	CVE-2016-7911	CVE-2016-7912	CVE-2016-7913
CVE-2016-7914	CVE-2016-7915	CVE-2016-7916	CVE-2016-7917	CVE-2016-8391
CVE-2016-8392	CVE-2016-8393	CVE-2016-8394	CVE-2016-8395	CVE-2016-8397
CVE-2016-8398	CVE-2016-8400	CVE-2016-8401	CVE-2016-8402	CVE-2016-8403
CVE-2016-8404	CVE-2016-8406	CVE-2016-8407	CVE-2016-8408	CVE-2016-8409
CVE-2016-8410	CVE-2016-8412	CVE-2016-8413	CVE-2016-8414	CVE-2016-8415

Table 2-4: CVE Fixes from Sierra Linux Reference (Continued)

CVE-2016-8416	CVE-2016-8417	CVE-2016-8419	CVE-2016-8420	CVE-2016-8421
CVE-2016-8424	CVE-2016-8425	CVE-2016-8426	CVE-2016-8427	CVE-2016-8428
CVE-2016-8429	CVE-2016-8430	CVE-2016-8431	CVE-2016-8432	CVE-2016-8434
CVE-2016-8435	CVE-2016-8436	CVE-2016-8437	CVE-2016-8438	CVE-2016-8439
CVE-2016-8440	CVE-2016-8441	CVE-2016-8442	CVE-2016-8443	CVE-2016-8444
CVE-2016-8449	CVE-2016-8450	CVE-2016-8451	CVE-2016-8452	CVE-2016-8453
CVE-2016-8454	CVE-2016-8455	CVE-2016-8456	CVE-2016-8457	CVE-2016-8458
CVE-2016-8459	CVE-2016-8460	CVE-2016-8461	CVE-2016-8463	CVE-2016-8464
CVE-2016-8465	CVE-2016-8466	CVE-2016-8468	CVE-2016-8469	CVE-2016-8473
CVE-2016-8474	CVE-2016-8475	CVE-2016-8476	CVE-2016-8477	CVE-2016-8478
CVE-2016-8479	CVE-2016-8480	CVE-2016-8481	CVE-2016-8483	CVE-2016-8632
CVE-2016-8633	CVE-2016-8636	CVE-2016-8645	CVE-2016-8646	CVE-2016-8655
CVE-2016-8658	CVE-2016-8660	CVE-2016-8666	CVE-2016-9083	CVE-2016-9084
CVE-2016-9120	CVE-2016-9178	CVE-2016-9313	CVE-2016-9555	CVE-2016-9576
CVE-2016-9588	CVE-2016-9644	CVE-2016-9685	CVE-2016-9754	CVE-2016-9755
CVE-2016-9756	CVE-2016-9777	CVE-2016-9793	CVE-2016-9794	CVE-2016-9806
CVE-2016-9919	CVE-2017-0306	CVE-2017-0307	CVE-2017-0325	CVE-2017-0327
CVE-2017-0328	CVE-2017-0329	CVE-2017-0330	CVE-2017-0331	CVE-2017-0332
CVE-2017-0333	CVE-2017-0334	CVE-2017-0335	CVE-2017-0336	CVE-2017-0337
CVE-2017-0338	CVE-2017-0339	CVE-2017-0403	CVE-2017-0404	CVE-2017-0427
CVE-2017-0428	CVE-2017-0429	CVE-2017-0430	CVE-2017-0432	CVE-2017-0433
CVE-2017-0434	CVE-2017-0435	CVE-2017-0436	CVE-2017-0437	CVE-2017-0438
CVE-2017-0439	CVE-2017-0440	CVE-2017-0441	CVE-2017-0442	CVE-2017-0443
CVE-2017-0444	CVE-2017-0445	CVE-2017-0446	CVE-2017-0447	CVE-2017-0448
CVE-2017-0449	CVE-2017-0451	CVE-2017-0452	CVE-2017-0453	CVE-2017-0454
CVE-2017-0455	CVE-2017-0456	CVE-2017-0457	CVE-2017-0458	CVE-2017-0459
CVE-2017-0460	CVE-2017-0461	CVE-2017-0462	CVE-2017-0463	CVE-2017-0464
CVE-2017-0465	CVE-2017-0507	CVE-2017-0508	CVE-2017-0510	CVE-2017-0516
CVE-2017-0518	CVE-2017-0519	CVE-2017-0520	CVE-2017-0521	CVE-2017-0523
CVE-2017-0524	CVE-2017-0525	CVE-2017-0526	CVE-2017-0527	CVE-2017-0528
CVE-2017-0531	CVE-2017-0533	CVE-2017-0534	CVE-2017-0535	CVE-2017-0536
CVE-2017-0537	CVE-2017-0561	CVE-2017-0563	CVE-2017-0564	CVE-2017-0567

Table 2-4: CVE Fixes from Sierra Linux Reference (Continued)

CVE-2017-0568	CVE-2017-0569	CVE-2017-0570	CVE-2017-0571	CVE-2017-0572
CVE-2017-0573	CVE-2017-0574	CVE-2017-0575	CVE-2017-0576	CVE-2017-0577
CVE-2017-0579	CVE-2017-0580	CVE-2017-0581	CVE-2017-0582	CVE-2017-0583
CVE-2017-0584	CVE-2017-0585	CVE-2017-0586	CVE-2017-0606	CVE-2017-0607
CVE-2017-0608	CVE-2017-0609	CVE-2017-0610	CVE-2017-0611	CVE-2017-0612
CVE-2017-0613	CVE-2017-0614	CVE-2017-0619	CVE-2017-0620	CVE-2017-0621
CVE-2017-0622	CVE-2017-0623	CVE-2017-0624	CVE-2017-0626	CVE-2017-0627
CVE-2017-0628	CVE-2017-0629	CVE-2017-0630	CVE-2017-0631	CVE-2017-0632
CVE-2017-0633	CVE-2017-0634	CVE-2017-0648	CVE-2017-0650	CVE-2017-0651
CVE-2017-1000111	CVE-2017-1000112	CVE-2017-1000251	CVE-2017-1000253	CVE-2017-1000363
CVE-2017-1000364	CVE-2017-1000371	CVE-2017-1000379	CVE-2017-1000380	CVE-2017-1000405
CVE-2017-10661	CVE-2017-10662	CVE-2017-10663	CVE-2017-10810	CVE-2017-10911
CVE-2017-11176	CVE-2017-11472	CVE-2017-11473	CVE-2017-12146	CVE-2017-12168
CVE-2017-12190	CVE-2017-12192	CVE-2017-12762	CVE-2017-13686	CVE-2017-13693
CVE-2017-13694	CVE-2017-13695	CVE-2017-13715	CVE-2017-14051	CVE-2017-14106
CVE-2017-14140	CVE-2017-14156	CVE-2017-14340	CVE-2017-14489	CVE-2017-14497
CVE-2017-14954	CVE-2017-14991	CVE-2017-15102	CVE-2017-15115	CVE-2017-15116
CVE-2017-15126	CVE-2017-15127	CVE-2017-15128	CVE-2017-15129	CVE-2017-15274
CVE-2017-15299	CVE-2017-15306	CVE-2017-15537	CVE-2017-15649	CVE-2017-15868
CVE-2017-15951	CVE-2017-16525	CVE-2017-16526	CVE-2017-16527	CVE-2017-16528
CVE-2017-16529	CVE-2017-16530	CVE-2017-16531	CVE-2017-16532	CVE-2017-16533
CVE-2017-16534	CVE-2017-16535	CVE-2017-16536	CVE-2017-16537	CVE-2017-16538
CVE-2017-16643	CVE-2017-16644	CVE-2017-16645	CVE-2017-16646	CVE-2017-16647
CVE-2017-16648	CVE-2017-16649	CVE-2017-16650	CVE-2017-16911	CVE-2017-16912
CVE-2017-16913	CVE-2017-16914	CVE-2017-16939	CVE-2017-16994	CVE-2017-17052
CVE-2017-17053	CVE-2017-17448	CVE-2017-17449	CVE-2017-17450	CVE-2017-17558
CVE-2017-17712	CVE-2017-17805	CVE-2017-17806	CVE-2017-17807	CVE-2017-17852
CVE-2017-17853	CVE-2017-17854	CVE-2017-17855	CVE-2017-17856	CVE-2017-17857
CVE-2017-17862	CVE-2017-17863	CVE-2017-17864	CVE-2017-17975	CVE-2017-18017
CVE-2017-18075	CVE-2017-18079	CVE-2017-18174	CVE-2017-18193	CVE-2017-18200
CVE-2017-18202	CVE-2017-18203	CVE-2017-18204	CVE-2017-18208	CVE-2017-18218
CVE-2017-18221	CVE-2017-18222	CVE-2017-18241	CVE-2017-18249	CVE-2017-18255

Table 2-4: CVE Fixes from Sierra Linux Reference (Continued)

CVE-2017-18257	CVE-2017-18261	CVE-2017-18270	CVE-2017-18344	CVE-2017-18360
CVE-2017-18379	CVE-2017-18509	CVE-2017-18549	CVE-2017-18550	CVE-2017-18551
CVE-2017-18552	CVE-2017-18595	CVE-2017-2596	CVE-2017-2634	CVE-2017-2647
CVE-2017-2671	CVE-2017-5546	CVE-2017-5547	CVE-2017-5548	CVE-2017-5549
CVE-2017-5550	CVE-2017-5551	CVE-2017-5576	CVE-2017-5577	CVE-2017-5669
CVE-2017-5897	CVE-2017-5967	CVE-2017-5970	CVE-2017-5972	CVE-2017-5986
CVE-2017-6001	CVE-2017-6214	CVE-2017-6345	CVE-2017-6346	CVE-2017-6347
CVE-2017-6348	CVE-2017-6353	CVE-2017-6874	CVE-2017-7187	CVE-2017-7261
CVE-2017-7273	CVE-2017-7277	CVE-2017-7294	CVE-2017-7308	CVE-2017-7346
CVE-2017-7374	CVE-2017-7477	CVE-2017-7487	CVE-2017-7495	CVE-2017-7533
CVE-2017-7541	CVE-2017-7542	CVE-2017-7616	CVE-2017-7618	CVE-2017-7645
CVE-2017-7889	CVE-2017-7895	CVE-2017-8061	CVE-2017-8062	CVE-2017-8063
CVE-2017-8064	CVE-2017-8065	CVE-2017-8066	CVE-2017-8067	CVE-2017-8068
CVE-2017-8069	CVE-2017-8070	CVE-2017-8071	CVE-2017-8072	CVE-2017-8106
CVE-2017-8797	CVE-2017-8831	CVE-2017-8890	CVE-2017-8924	CVE-2017-8925
CVE-2017-9059	CVE-2017-9074	CVE-2017-9075	CVE-2017-9076	CVE-2017-9077
CVE-2017-9150	CVE-2017-9211	CVE-2017-9242	CVE-2017-9605	CVE-2017-9984
CVE-2017-9985	CVE-2017-9986	CVE-2018-1000028	CVE-2018-1000199	CVE-2018-10087
CVE-2018-10124	CVE-2018-1066	CVE-2018-10675	CVE-2018-10901	CVE-2018-1091
CVE-2018-10938	CVE-2018-11232	CVE-2018-11506	CVE-2018-12714	CVE-2018-12928
CVE-2018-12929	CVE-2018-12930	CVE-2018-12931	CVE-2018-13096	CVE-2018-13099
CVE-2018-13405	CVE-2018-13406	CVE-2018-14619	CVE-2018-14634	CVE-2018-14641
CVE-2018-14646	CVE-2018-14678	CVE-2018-16276	CVE-2018-16597	CVE-2018-16862
CVE-2018-16880	CVE-2018-16882	CVE-2018-16885	CVE-2018-17182	CVE-2018-17977
CVE-2018-18386	CVE-2018-18445	CVE-2018-18955	CVE-2018-20449	CVE-2018-20509
CVE-2018-20510	CVE-2018-20784	CVE-2018-20836	CVE-2018-20961	CVE-2018-25015
CVE-2018-5332	CVE-2018-5333	CVE-2018-5344	CVE-2018-5703	CVE-2018-5750
CVE-2018-5803	CVE-2018-5814	CVE-2018-5953	CVE-2018-5995	CVE-2018-6927
CVE-2018-7191	CVE-2018-7480	CVE-2018-7492	CVE-2018-7566	CVE-2018-8781
CVE-2018-9568	CVE-2019-0145	CVE-2019-10125	CVE-2019-10126	CVE-2019-10140
CVE-2019-10142	CVE-2019-10220	CVE-2019-11190	CVE-2019-11487	CVE-2019-11683
CVE-2019-11810	CVE-2019-11815	CVE-2019-12615	CVE-2019-12881	CVE-2019-13272

Table 2-4: CVE Fixes from Sierra Linux Reference (Continued)

CVE-2019-14835	CVE-2019-14897	CVE-2019-14898	CVE-2019-14901	CVE-2019-15099
CVE-2019-15239	CVE-2019-15292	CVE-2019-15504	CVE-2019-15505	CVE-2019-15538
CVE-2019-15791	CVE-2019-15792	CVE-2019-15793	CVE-2019-15794	CVE-2019-15902
CVE-2019-15916	CVE-2019-15918	CVE-2019-15925	CVE-2019-15926	CVE-2019-15927
CVE-2019-16229	CVE-2019-16230	CVE-2019-16231	CVE-2019-16232	CVE-2019-16233
CVE-2019-16234	CVE-2019-16746	CVE-2019-16995	CVE-2019-17133	CVE-2019-17666
CVE-2019-18198	CVE-2019-18675	CVE-2019-18680	CVE-2019-18805	CVE-2019-18810
CVE-2019-18812	CVE-2019-18813	CVE-2019-19044	CVE-2019-19048	CVE-2019-19050
CVE-2019-19052	CVE-2019-19053	CVE-2019-19060	CVE-2019-19061	CVE-2019-19069
CVE-2019-19070	CVE-2019-19071	CVE-2019-19074	CVE-2019-19075	CVE-2019-19078
CVE-2019-19079	CVE-2019-19318	CVE-2019-19319	CVE-2019-19377	CVE-2019-19378
CVE-2019-19447	CVE-2019-19449	CVE-2019-19768	CVE-2019-19807	CVE-2019-19813
CVE-2019-19814	CVE-2019-19815	CVE-2019-19816	CVE-2019-19927	CVE-2019-20794
CVE-2019-20934	CVE-2019-25044	CVE-2019-3837	CVE-2019-3874	CVE-2019-3887
CVE-2019-3896	CVE-2019-3901	CVE-2019-8912	CVE-2019-8956	CVE-2019-8980
CVE-2019-9003	CVE-2019-9162	CVE-2019-9213	CVE-2019-9500	CVE-2020-10773
CVE-2020-11884	CVE-2020-12351	CVE-2020-12352	CVE-2020-13974	CVE-2020-14304
CVE-2020-14305	CVE-2020-14356	CVE-2020-15852	CVE-2020-25220	CVE-2020-25221
CVE-2020-25668	CVE-2020-25669	CVE-2020-27786	CVE-2020-27815	CVE-2020-27825
CVE-2020-28588	CVE-2020-29534	CVE-2020-29569	CVE-2020-29661	CVE-2020-35513
CVE-2020-35519	CVE-2020-36387	CVE-2020-7053	CVE-2020-8428	CVE-2020-8835
CVE-2020-9391	CVE-2021-20194	CVE-2021-20261	CVE-2021-21781	CVE-2021-22555
CVE-2021-26708	CVE-2021-26934	CVE-2021-28039	CVE-2021-28375	CVE-2021-28660
CVE-2021-28691	CVE-2021-29154	CVE-2021-29266	CVE-2021-31440	CVE-2021-32606
CVE-2021-33200	CVE-2021-33909	CVE-2021-34866	CVE-2021-3489	CVE-2021-3490
CVE-2021-3491	CVE-2021-35039	CVE-2021-3715	CVE-2021-3743	CVE-2021-37576
CVE-2021-3760	CVE-2021-38300	CVE-2021-4028	CVE-2021-4093	CVE-2021-41073
CVE-2021-4154	CVE-2021-4157	CVE-2021-43056	CVE-2021-43057	CVE-2021-43267
CVE-2022-0185	CVE-2022-0500	CVE-2022-0646	CVE-2022-0742	CVE-2022-0847
CVE-2022-0995	CVE-2022-0998	CVE-2022-1043	CVE-2022-1055	CVE-2022-1116
CVE-2022-1158	CVE-2022-1280	CVE-2022-1516	CVE-2022-1678	CVE-2022-1679
CVE-2022-1729	CVE-2022-1786	CVE-2022-1974	CVE-2022-1975	CVE-2022-1976

Table 2-4: CVE Fixes from Sierra Linux Reference (Continued)

CVE-2022-1998	CVE-2022-20105	CVE-2022-20106	CVE-2022-20107	CVE-2022-20108
CVE-2022-23222	CVE-2022-24122	CVE-2022-25636	CVE-2022-2590	CVE-2022-2938
CVE-2022-2964	CVE-2022-2978	CVE-2022-3061	CVE-2022-3103	CVE-2022-3169
CVE-2022-3170	CVE-2022-3238	CVE-2022-33743	CVE-2022-34918	CVE-2022-3524
CVE-2022-3541	CVE-2022-3577	CVE-2022-3625	CVE-2022-3628	CVE-2022-3643
CVE-2022-38096	CVE-2022-38457	CVE-2022-3903	CVE-2022-3910	CVE-2022-3977
CVE-2022-40133	CVE-2022-41674	CVE-2022-4269	CVE-2022-42719	CVE-2022-42720
CVE-2022-42721	CVE-2022-42722	CVE-2022-4696	CVE-2022-47938	CVE-2022-47939
CVE-2022-47940	CVE-2022-47941	CVE-2022-47942	CVE-2022-47943	CVE-2022-47946
CVE-2022-4842	CVE-2023-0122	CVE-2023-0597	CVE-2023-23586	CVE-2023-26544
CVE-2023-26605	CVE-2023-26606	CVE-2023-26607		

2.4 Known Issues

The following table presents the known issues in this release.

ID	Description	Impacted Domain
QTI9X07-5568	[AUDIO][AVCFG] Some AV logs are missing in QXDM	Some AV logging configuration are not available in the latest QXDM logger.
QTI9X07-5795	[AVMS] Cannot install the software application successfully when power cycle during download progress	This issue will not affect module operation and SOTA can manually install after module reboot.
QTI9X07-5298	[MM][FLOG] No data is returned when checking to FLOG entries	No impact on customer side, only on RD module debugging.
QTI9X07-5783	[USB-SS] The module does not wake up from suspend mode when sending the AT command in the first attempt	It only impacts WP7605 and can be recovered by sending again.
QTI9X07-3655	Firmware update using xmodem protocol over USB modem interface is not successful. Firmware installation eventually failed after the firmware is successfully downloaded. This issue has been fixed in modem firmware SWI9X07Y_02.37.07.00, but this modem firmware is not included in any firmware release packages	Using AT+WFWUPD=1 to perform FW update with XMODEM protocol fails. The issue is seen after SWI9X07Y_02.29.01.00.
QTI9X07-4912	With R2C SIM V5.x, EF_OPLMNwAct is not taken into account after SIM REFRESH	With R2C SIM V5.x, EF_OPLMNwAct is not taken into account after SIM REFRESH.
LE-8872	The value of object /7/0/0 (SMS Tx counter) is not updated when using AT Command to send SMS	Customer is unable to see statistic when sending SMS successfully.

2.5 Major Configuration Changes

This section presents the major carrier configuration changes in this release.

Table 2-5: Generic

Approved FW	Configuration	ID	Description
SWI9X07Y_02.37.06.05	v002_128_000	OEMPRI-28158	Change back WP76xx GENERIC R17 main branch to non-GCF branch. Use 02.37.06.05 and change back PRI build version to 000.

..

Table 2-6: Verizon

Approved FW	Configuration	ID	Description
SWI9X07Y_02.37.06.05	v002.123_000	OEMPRI-26386	Update Firmware to SWI9X07Y_02.37.06.05

A: Appendix

A.1 Abbreviations and Definitions

Abbreviation / Acronym	Definitions
AT	Access Terminal, Attention
CS	Circuit Switched
EDL	Emergency Download
FDT	Firmware Download Tool
GCF	Global Certification Forum
LK	Little Kernel Linux bootloader
MCU	Microcontroller Unit – An onboard MCU enables Ultra Low Power modes of operation
MR	Maintenance Release
PSM	Power Saving Mode
QMI	Qualcomm Messaging Interface
SDP	Software Download Protocol
ULPM	Ultra Low Power Mode

A.2 Related Documentation

- WP76xx - Product Technical Specification
  Reference number: 4119652
- WPx5xx-76xx-77xx AT Command Reference
  Reference number: 4118047
- WP Series - Preparing Your Devices for Deployment
  Reference number: 41110380
- WPX5-76-77 Scalability Guide
  Reference number: 41110866
- WP Series - Secure Boot
  Reference number: 41112164