Texas Instruments Incorporated

WL18xx BT Service Pack 4.7

Release Notes
Revision 1.0

May 20, 2021

Please be aware that an important notice concerning availability, standard warranty, and use in critical applications of Texas Instruments semiconductor products and disclaimers thereto appears at the end of this data sheet.

1. Service Pack Information

Filename	TIInit_11.8.32.bts
Version	Service Pack 4.7
Compatibility	For usage with WL18xx 2.2, 2.1 (WL18XXGYFVR, WL18XXGHYFVR) and WL18xx modules (WL1831MOD, WL1835MOD, WL1837MOD).
Comments	This service pack is based on internal version 148

1.1. General Information

The script is required to be run after device power up.

1.2. Included files

This service pack includes the following:

- Release notes
- Service pack script
- XML library for usage with HCITester, Logger and ScriptPad
- ILI configuration file for Logger tool

1.3. Wakeup settling time configuration

Please note that default wakeup settling time is 30ms. The Service Pack reduces the settling time to 5ms, equal to the same settling time value set by WLAN. Please note that if default values are required to be changed, both values must be updated.

1.4. ANT

Please contact your local customer representative for information regarding ANT licensing and support.

2. Updated Fixes in Service Pack 4.7

2.1. Fix a bug in Impersonation in Passkey entry protocol (CVE-2020-26558)

This service pack release fixes a security bug in Passkey entry protocol. This attack leverages a reflection attack on a device initiating a Passkey pairing procedure to acquire information on all the bits selected by the initiator to respond correctly to a device in the Responder role with the bits observed by a user. The fix ensures that the when the peer's public key matches with the local public key, the authentication is aborted. Please refer to CVE-2020-26558 for further details.

Note: Please, use the BTS file "TIInit_11.8.32-BT4.2.bts" For BT4.2 TIBluetopiaPM stack. This BTS file contains two VS commands to set FW core version to 4.2 to be compatible with 4.2 BluetopiaPM stack.

3. Updated Fixes in Service Pack 4.6

3.1. Support for BT5.1

This service pack also contains the fixes for BT5.1 certification. Please, refer to the QDID 156966, 156961, 156957 for BT5.1 certification.

https://launchstudio.bluetooth.com/ListingDetails/RedirectFromQdid/156966
https://launchstudio.bluetooth.com/ListingDetails/RedirectFromQdid/156961
https://launchstudio.bluetooth.com/ListingDetails/RedirectFromQdid/156957

Note: Please, use the BTS file "TIInit_11.8.32-BT4.2.bts" For BT4.2 TIBluetopiaPM stack. This BTS file contains two VS commands to set FW core version to 4.2 to be compatible with 4.2 BluetopiaPM stack.

4. Updated Fixes in Service Pack 4.5

4.1. Fix a bug in LE scan for ADV_IND and SCN_RSP (CVE-2019-15948)

This service pack release fixes a security bug in the logic of LE scan activity that could potentially allow a remote attacker to trigger a buffer overflow in the Bluetooth firmware by injecting malformed ADV_IND and SCN_RSP packets. This service pack fixes this vulnerability by detecting such malformed packets and discarding them, effectively disallowing any such overflow attack. For more information, please refer to CVE-2019-15948.

5. Updated Fixes in Service Pack 4.4

5.1. BR/EDR minimum Encryption Key Size update

This service pack release updates default value of minimum LMP encryption key size to 7 octets to comply with the Bluetooth Expedited Errata Correction 11838. The minimum LMP encryption key size was set to 5 octets by default in older releases.

6. Updated Fixes in Service Pack 4.3

6.1. Public Key Validation for BR/EDR Secure Simple Pairing (SSP)

This service pack validates the public key received over the air when pairing a new BR/EDR device using the Secure Simple Pairing (SSP). This security enhancement provides additional protection against certain man-in-the-middle type of attacks.

6.2. Fix Disconnection due to peer sniff attempt of 1

The BT classic connection may get disconnected with error code (0x08 - Connection Timeout) when the peer device sends sniff request with sniff attempt 1 and the local WL18xx controller is the slave in the connection. This service pack fixes this bug by renegotiating sniff attempt of 4 with the peer device so the connection timeout does not happen.

7. Updated Fixes in Service Pack 4.2

7.1. LE Scan

There could be a race condition where LE scan didn’t stop after issuing LE stop command. This resulted in inability to establish further LE scan commands. Issue is resolved in current service pack.

7.2. BT Spec version

WL8 device now advertises support of BT spec 4.2.

8. Updated Fixes in Service Pack 4.1

8.1. Device lockup during initialization

There could be a race condition during initialization sequence when working in high UART baud rates, leading to device lockup. Issue is resolved in current service pack only for the non TTR (Test Time Reduction) version.

9. Updated Fixes in Service Pack 4.0

9.1. Unaligned WBS support

Added support for unaligned WBS.

9.2. BT-BLE-ANT lockup

Under extream test condition of BT BLE and ANT activities, the device could reach a lockup state. Issue is resolved in this service pack.

10. Updated Fixes in Service Pack 3.9

10.1. Initialization lock up

There could be a rare lock up of the device if add-ons commands were executed right after “Send_HCI_VS_Stop_VS_Lock 0xFE38” without waiting for command complete. Issue is resolved in current service pack [OMAPS00316960]

10.2. PCM clock extension

PCM clock extension might have not functioned correctly after repeated attempts of connecting/disconnecting a voice connection with minimal delay between attempts. Issue is resolved in current service pack [OMAPS00325111]

10.3. Simultaneous connection attempt from both sides

Attempting to create connection from both local and peer device and same time may have resulted in unsuccessful connection. Issue is resolved in current service pack [OMAPS00326896]

10.4. LE connection lock up

There could be a rare lock up of the device during LE connection, if both master and slave terminated the connection right at the same time, and device’s role was master. Issue is resolved in current service pack [OMAPS00322971]

11. Updated issues in Service Pack 3.8

11.1. Unsuccessful connection

In certain occasions, upon removing HFP, connection could not be established when initiated from the host. Issue was introduced in service pack 3.4, and is resolved in current service pack.

11.2. Missing link key event

Upon removing link key from peer (phone), controller should send missing link key event to the host, rather than automatically establishing a secured connection – Issue is resolved in current service pack.

11.3. Unsuccessful connection to iPhone 6

Upon disabling switch request from the host, the iPhone requests continuously switch request during authentication procedure. TI's controller returns "not accepted" with reason "collision". As a result, the iPhone returns collision upon LMP IO capability request. To solve that, TI's controller now returns reason code "not accepted" rather than "collision". Issue is resolved in current service pack.

11.4. WBS

WBS audio quality optimization. Fixed audio ticks.

11.5. BT WLAN coexistence

Rx timing calibration might have failed upon initializing WLAN and BT at the same time. Issue is resolved in current service pack (new PHY section in the Initscript).

11.6. BT WLAN coexistence

HCI might become unresponsive if WLAN was active and BT was being initialized. This resulted due to BT reaching an erroneous continuous interrupt mode. Issue is resolved in current service pack.

12. Updated issues in Service Pack 3.7

12.1. BER – new and updated API's

Reset BER API: Send_HCI_VS_DRP_Reset_BER_Meter 0xFE29
Added in order to reset the BER counters.

Read BER Meter status: Send_HCI_VS_DRP_Read_BER_Meter_Status 0xFE2A
Opcode has changed for version compatibility

12.2. Collision between local power control and peer transaction

During simple pairing with a peer, the DUT has sent a power control local transaction, which resulted in disconnection. Issue is resolved in current service pack.

12.3. Increased interval between two BLE slaves

When a BLE master has two slaves the system tries to optimize the power consumption and schedules them back to back with one frame between them, and can stay more time in low power mode.

Due to this power optimization, if the first BLE slave wants to send more data (continuation bit) the performance of the second BLE slave was compromised.

By increasing the interval between the slaves, the issue was resolved and the low power optimization was maintained.

12.4. Voice over HCI stability

In order to use voice over HCI the system had to be pre-configured and couldn't configure dynamically the voice settings. The issue was fixed and currently the voice settings can be configured dynamically either over HCI or not.

12.5. BT ACL link priority is set higher in case of starvation by the WLAN IP

Added a mechanism to change the priority of ACL links in case they are being starved by the WLAN IP. This mechanism will only take effect if WLAN FW version 8.9.0.0.35 or newer is used.

12.6. WLAN sensitivity degradation

WLAN Rx performance may be degraded when testing WLAN in non-operational mode. Issue is resolved in current service pack.

13. Updated issues in Service Pack 3.6.1

13.1. Initscript may not load successfully at high baud rates

Fixed an issue, which was introduced in service pack 3.6, where Initscript was not loaded successfully in high baud rates.

14. Updated issues in Service Pack 3.6

14.1. Revised implementation of Pairing failed due to LMP response timeout (previously done in SP3.5)

This service pack has the fix for a transaction collision between Packet Type Table request and other transactions. This fix no longer includes rejecting Packet type Table request with reason collision.

15. Updated issues in Service Pack 3.5

15.1. Pairing failed due to LMP response timeout

Fixed a transaction collision between Packet Type Table request and other transactions.
This fix includes rejecting Packet type Table request with reason collision, it is assumed stack requiring modified packet type table will re-issue command until success.

15.2. WiFi-Zigbee coex, Zigbee would be blocked once Bluetooth init script was run

Bluetooth init script took control of hardware pins controlling WLAN-Zigbee coex.

15.3. WiFi-BT coex, WLAN provided channel map was ignored in noisy environment (lots of interference)

Change the WLAN reported channel map priority to be higher than local classification and peer classification channel maps.

15.4. ANT receive statistics degraded occasionally when running long runs

Periodic calibrations did not take ANT or running connections into account.

15.5. When running BLE connection and receiving unknown LL command, connection would drop

Upon reception of un-known LL command (when working with new device or due to peer side error) the received buffer was not cleared.

15.6. Add option to keep PCM clock on after voice connection removal

Host can configure PCM lines to remain on, this is typically used when WL8 PCM clock drives external components such as DSP.

To enable this feature, add the following command to init script (write UINT16 value 0xCAFE to address 0x2004012C).

```
# Tell controller to keep PCM clock on after voice removal by writing 0xCAFE,
# any other value will allow controller to turn off PCM clock upon voice channel removal
# duration set by register 0x20086A1E (UINT16 value)
Send_HCI_VS_Write_Memory 0xFF03, 0x2004012C, 02, 0xCAFE
Wait_HCI_Command_Complete_VS_Write_Memory_Event 5000, any, HCI_VS_Write_Memory, 0x00

# Tell controller the time duration (from voice connection removal) to keep PCM clock on
# 0 means keep on forever
# any other value between 0x0001 and 0xFFFF are time value in units of 100mS
# e.g. value 10 means 10*100mS=1 second
Send_HCI_VS_Write_Memory 0xFF03, 0x20086A1E, 02, 0x0000
Wait_HCI_Command_Complete_VS_Write_Memory_Event 5000, any, HCI_VS_Write_Memory, 0x00
```

15.7. When running BLE scan + Page scan + Inquiry scan + Inquiry, after a prolonged running time the inquiry would not get responses.

Prevent race condition around register setting when entering / exiting deep sleep.

15.8. Connection drops (few times in 24 hours) when connect as slave in sniff with sniff interval of 500mS.

Prevent race condition in internal scheduler between channel classification mechanism and mode transitions between sniff and active.

15.9. Internal BER METER command enhancements

Added new interface commands to read BER meter status.

16. Updated issues in Service Pack 3.4

16.1. Change BT LMP and HCI version to indicate BT core spec 4.1 support

Updated LMP core version and HCI version to 4.1
In order to achieve backwards compatibility with old versions of StoneStreetOne stacks, who are not willing to work with controllers supporting BT Core spec 4.1, a method was provided to revert this change as part of init script, and have controller continue reporting BT Core spec 4.0.

16.2. Role switch (master to slave roles) failure when slot offset value was 0uS

When role switching from master to slave, and peer slot offset value was 0uS, role switch often failed.

16.3. WLAN transmission EVM degraded after Bluetooth power up due to shared power management configuration

At Bluetooth power up, the shared DC2DC configuration was changed in a manner that degraded WLAN transmission EVM.

16.4. Inquiry success statistics reduced once connected to an A2DP headset (even without streaming)

Once connected to an A2DP headset, when performing Inquiry, success rates (number of results) was lower than when not connected to the A2DP headset, this was seen even if headset was not streaming audio. Implementation was changed to recognize actual streaming state instead of creation of channel.

16.5. Controller did not go into low power mode (deep sleep) during sniff if link supervision timeout was shortened to 5 seconds (OMAPS00308441)

When setting Link Supervision Timeout to 5 seconds and observing current consumption, it was noticed that device did not switch to low power mode and remained in awake mode, thus drawing higher current.

16.6. Pairing failure due to LMP collision when performing SDP prior to encryption setup (OMAPS00309308)

When attempting to pair with Nexus4 and a stack which performed SDP as soon as connection started, a collision between peer initiated Packet Type Table Request and peer initiated IO Capability request caused pairing to fail.

16.7. BT slave connection drops when running full BW ANT search

When running ANT high duty cycle search, Bluetooth connections in the slave role occasionally dropped connection.

16.8. Two “Connection complete events” to peer same device

When TI BT device would page peer and peer would page BT device at same time, occasionally two connection complete events were received, it could be with success on two handles (same peer BD address) or success on one and page timeout on the other.

16.9. ACL connection dropped (with reason LMP response timeout) on peer initiated sniff sub-rate followed immediately by peer initiated exit sniff (OMAPS003086646).

When peer initiated sniff sub-rate and then immediately initiated exit sniff, a collision would occur between the requests and ACL connection would drop with reason LMP_Respose_Timeout.

16.10. Device gets stuck while streaming A2DP and performing remote name request (OMAPS00307325).

When performing remote name request while streaming A2DP, device sometimes gets stuck.

17. Updated issues in Service Pack 3.3

17.1. Low A2DP streaming quality (OMAPS00299958)

During A2DP streaming, if the host tries connecting to a 2nd device and cancels it by issuing HCI_Create_Connection_Cancel command, data streaming throughput with A2DP peer drops and stays low. Issue is resolved in current service pack

17.2. ETSI 300 328 version 1.8.1 (OMAPS00303077)

ETSI 300 328 version 1.8.1 frequency hopping adaptively test fails. Issue is resolved in current service pack.

17.3. LMP Feature Request collision (OMAPS00300104)

When in Master role, some BT controllers send LMP_Feature_Request prior to LMP connection setup messages (right after the POLL-NULL sequence, before the master is sending any LMP). TI controller response to peer initiated LMP_Feature_Request with LMP_Not_accepted and reason invalid parameter, which causes peer device to crash and connection to drop. We have modified the response reason to bypass peer crash.

17.4. Applying Tester_Packet_TX_RX in a loop causes corrupted transmission

When applying HCI_VS_DRPb_Tester_Packet_TX_RX in a loop, the transmission was corrupted. Issue is resolved in current service pack.

17.5. Multiple BLE connections

Optimized scheduling in multiple BLE connections.

17.6. Reduce BLE power

Reduce BLE transmission level by ~2dB to meet regulatory requirements (FCC).

17.7. Initscript download failes (OMAPS00304315)

Initscript would not pass (RTS stuck high for ~5 minutes) when setting UART BAUD rate to 400kbps.

18. Updated issues in Service Pack 3.2

18.1. Initscript download fails (OMAPS00296623)

On PG2.2 devices the device wakes up with PLL disabled (older devices had PLL enabled by default). As part of PLL enable sequence, the clock tree is modified including the clocks and dividers of host interface UART, this version halts host interface (by raising RTS) during the PLL activation process.

18.2. Voice over HCI Interface Support

SP3.2 adds voice over HCI (UART) support; control over HCI/PCM channel is done through a VS command, for more details, please refer to *SWRU303B_WL18xx_VS_Specific_HCI_Cmds*

18.3. BT HID (mouse) get stuck/lag during BT scan (OMAPS00295839)

A fix in scheduling mechanism solving a collision between inquiry/page and inquiry scan/page scan in the presence of sniff. When page scan/inquiry scan window started (registered to start) exactly at sniff instance, it was queued into same list that inquiry/page would be inserted into. Once sniff instance ended, the arbitration between page / inquiry and page scan/inquiry scan was done incorrectly removing and re-inserting inquiry into head of queue in a loop.
During this time none of the activates performed properly. This version corrects the arbitration between page/inquiry and page scan/inquiry scan by inserting page/inquiry at end of "todo" queue.

19. Updated issues in Service Pack 3.1

19.1. Quality of Service during A2DP

A bug in an internal algorithm which optimizes the QoS of A2DP streams was fixed. Current change is an improvement of previous fix included in Service Pack 2.6 [MCS00124783].

19.2. Device stuck during ACL data connection with GPS

In some cases the device may get stuck due to a race between receiving Bluetooth ACL packet from Host and GPS data packet. Issue has been resolved in current service pack. [MCS00124630]

19.3. BT PLL operation before WLAN ON

In a corner case of strong device process some chips wake-up sequence (above 75 degrees) do not function correctly when BT PLL is turned ON before WLAN PLL. [MCS00124819].

20. Updated issues in Service Pack 3.0

20.1. Quality of Service during A2DP

Automatic sending of QOS LMP during A2DP has been disabled. Quality of Service is required to be initiated by host stack as defined in BT specification.

21. Updated issues in Service Pack 2.9

21.1. BLE Advertise blocked

BLE advertise was blocked due to WLAN / BLE co-existence mechanism. Issue has been resolved in current service pack.

21.2. A2DP automatic stream recognition

Automatic A2DP stream recognition caused disconnection due to incorrect poll interval value issued with Quality of Service LMP.

22. Updated issues in Service Pack 2.8

22.1. A2DP Quality of Service during WLAN activity

In the case where QOS logic does not allow guaranteed link some headset peers disconnect A2DP profile if QOS is initially refused. To avoid such cases device will initially accept QOS requests. Issue has been resolved in current Service Pack. [MCS00121197]

22.2. Data abort during heavy WLAN VoIP

In some cases of WLAN VOIP with BT activity a data abort may occur due to inadequate resource allocation from shared resources causing an internal timeout. Issue has been resolved in current Service Pack. [MCS00122074]

23. Updated issues in Service Pack 2.7

23.1. HID & A2DP during WLAN

In some cases where A2DP stream is operating in parallel to BT 2 HID connections while WLAN is browsing, the device stops responding and BT reset is required [MCS00121536]

24. Updated issues in Service Pack 2.6

24.1. Short SNIFF during deep sleep enabled

Deep sleep clock compensation algorithm was not accurate and led to packet loss in the scenario of a short sniff interval. As result BT HID connection may disconnect due to LSTO. [MCS00120135].

24.2. A2DP Quality of Service (QoS)

A bug in an internal algorithm which optimizes the QoS of A2DP streams was fixed. The bug could lead to audio breaks in the A2DP stream, mainly in noisy environments [MCS00120848].

25. Updated issues in Service Pack 2.5

25.1. Changing of output power table configuration defaults

Power table defaults cannot be updated after initial service pack due to an issue in the updating mechanism. Issue will be fixed in service pack release.

26. Updated issues in Service Pack 2.3

26.1. BLE test mode workaround

Limitation has been removed: Due to a bug in the calibrations scheduling mechanism, periodic calibrations is required to be disabled before BLE test mode is activated. [MCS00113851]

26.2. Updated XML sleep mode vendor specific

Sleep mode configuration vendor specific command has been updated. ‘short deep sleep enable’ parameter has been changed to reserved. Please note that default value of 0 must be used. [MCS00113312]

27. Updated issues in Service Pack 2.2

27.1. Higher power during BLE advertise

Power consumption is high during BLE advertise, this limitation to be fixed in next service pack release.

28. Updated issues in Service Pack 2.1

28.1. Power Control Optimization

Golden range has been modified to improve interferer immunity in very noisy RF environments.

28.2. AFH Optimization

AFH mechanism has been modified to improve behavior during multiple interferer environments. In the case of all channels classified as channels for removal, AFH will refrain from removal of additional channels.

28.3. Improved BT/LE/ANT co-existence

BLE and ANT operation in parallel causes disconnections from time to time, scheduling has been optimized.

28.4. A3DP interruption

Due to a memory sharing violation of AVPR and MAIN CPU's, unpredictable exception occurred during A3DP connection.

28.5. High Sleep Current

Due to two digital hardware issues, a relatively high sleep current is seen. Issue has been resolved in this service pack.

28.6. Degradation of BT modulation due to LVDC2DC ripple

BT Modulation - some degradation in min deviation may be seen. Root cause for this degradation has been identified as coupling from the LVDC2DC to the BT core. Issue has been resolved in service pack.

28.7. High temperature performance

Connection instability has been detected on some devices during high temperatures. Hardware issue found and fix available in next hardware version. Issue has been resolved in service pack.

29. Limitations

29.1. Power vector lower limit

Power vectors are predefined in the service pack. Please note that in case of manual customization of power vectors, limitation of lower limit must be enforced. BT BR/BLE/ANT minimum output power may not be configured lower than -25dBm. BT EDR minimum output power may not be configured lower than -20dBm

29.2.

Important Notice

Texas Instruments and its subsidiaries (TI) reserve the right to make changes to their products or to discontinue any product or service without notice, and advise customers to obtain the latest version of relevant information to verify, before placing orders, that information being relied on is current and complete. All products are sold subject to the terms and conditions of sale supplied at the time of order acknowledgement, including those pertaining to warranty, patent infringement, and limitation of liability.

TI warrants performance of its semiconductor products to the specifications applicable at the time of sale in accordance with TI's standard warranty. Testing and other quality control techniques are utilized to the extent TI deems necessary to support this warranty. Specific testing of all parameters of each device is not necessarily performed, except those mandated by government requirements.

Certain applications using semiconductor products may involve potential risks of death, personal injury, or severe property or environmental damage ("Critical Applications"). TI SEMICONDUCTOR PRODUCTS ARE NOT DESIGNED, AUTHORIZED, OR WARRANTED TO BE SUITABLE FOR USE IN LIFE–SUPPORT DEVICES OR SYSTEMS OR OTHER CRITICAL APPLICATIONS. INCLUSION OF TI PRODUCTS IN SUCH APPLICATIONS IS UNDERSTOOD TO BE FULLY AT THE CUSTOMER'S RISK.

In order to minimize risks associated with the customer's applications, the customer to minimize inherent or procedural hazards must provide adequate design and operating safeguards.

TI assumes no liability for applications assistance or customer product design. TI does not warrant or represent that any license, either express or implied, is granted under any patent right, copyright, mask work right, or other intellectual property right of TI covering or relating to any combination, machine, or process in which such semiconductor products or services might be or are used. TI's publication of information regarding any third party's products or services does not constitute TI's approval, warranty or endorsement thereof.