

ENGINEERING Release Notes

BT850-Sx, BT851 and BT860-Sx

Version BCM20703A2_001.002.011.0332.03xx

January 2021

For access to this ENGINEERING firmware package / utilities – please contact our Technical Support team at support@lairdconnect.com

Release notes are a summary of new and enhanced features, resolved issues, and known issues that are not resolved in this firmware version. This release note describes the changes and enhancements to the firmware of the BT850 / BT851 and BT860 modules / Adapters utilizing Cypress CYW20704A2 silicon.

The firmware images are built by Cypress to meet Laird Connectivity's requirements and so the version number used utilises the Cypress formats. The firmware is identical between the 2 versions listed below, except for the main host interface being USB or UART respectively.

VERSION: BCM20703A2_001.002.011.0201.0332.0345 & .0344

TBC Release date – Engineering version January 2021

- **BT850 / BT851 - USB**
BCM20703A2_001.002.011.0332.0345
- **BT860 - UART**
BCM20703A2_001.002.011.0332.0334

CVE Related Updates

BCM20703A2-2206 CVE-2019-19193: check Invalid Connection Request BCM20703A2_001.002.011.0329.0000
BCM20703A2-2201 BT-CERT: Errata 11838 and 10734 Test cases failure fixes BCM20703A2_001.002.011.0322.0000, BCM20703A2_001.002.011.0321.0000
BCM20703A2-2196 CVE-2019-16336: Enforce LE-LL message length check BCM20703A2_001.002.011.0320.0000
BCM20703A2-2197 CVE-2019-17061: Check if receiving an LLID 0 packet can cause problems.
BCM20703A2-2174 11838 erratum:- when IUT acts as a master Encryption change event returns connected rejected due to Security reasons rather than success
BCM20703A2-2144 Implement Erratum 11838: Encryption Key Size Updates
BCM20703A2-2168 - Master: EIR buffer overflow / BT exploit CVE-2019-11516 BCM20703A2_001.002.011.0312.0000

Additional Updates and Bug Fixes

BCM20703A2-2184 Change default mode of LE Scan remap mechanism enhancement for COEX as disable.
BCM20703A2-2118 LE Scan remap mechanism enhancement for coex.
BCM20703A2-2139 LLCP version indication collision BCM20703A2_001.002.011.0306.0000
BCM20703A2-2135 android stack does not like zero length HCI ACL BCM20703A2_001.002.011.0305.0000
BCM20703A2-2109 Enable LE extended scan BCM20703A2_001.002.011.0301.0000
BCM20703A2-2092 BB/PROT/FLH/BV-02-C test case Fails BCM20703A2_001.002.011.0300.0000
BCM20703A2-2087 add new build target for USB_40MHz_WakeOnBle to build_all.mk BCM20703A2_001.002.011.0299.0000
BCM20703A2-2087 add new build target for USB_40MHz_WakeOnBle to build_all.mk
BCM20703A2-2087 create new build target for USB_40MHz_WakeOnBle BCM20703A2_001.002.011.0298.0000
BCM20703A2-2097 Fix bug with BATCH scan BCM20703A2_001.002.011.0297.0000
BCM20703A2-2084 Disable BATCH_SCAN as it's breaking PCF BCM20703A2_001.002.011.0296.0000
BCM20703A2-2074 Fix bug with BCM20703A2-1912 BCM20703A2_001.002.011.0292.0000
BCM20703A2-2053 Fix bug with FIX_CQ_SWWICED_8997 BCM20703A2_001.002.011.0283.0000
BCM20703A2-2014 Apply fix to all targets BCM20703A2_001.002.011.0278.0000
BCM20703A2-2024 Encryption status failure event incorrectly being passed up to the application BCM20703A2_001.002.011.0275.0000
BCM20703A2-2022 Disable FIX_CQ_SWWICED_8997 for specific customer
BCM20703A2-2002 BT 5.0 version report is wrong in LL_LE BCM20703A2_001.002.011.0270.0000
BCM20703A2-2001 Fix bug with BCM20703A2-1998
BCM20703A2-2000 Enable HW Pipeline AFH patches for wiced audio sink
BCM20703A2-1998 Disable BATCH_SCAN patch
BCM20703A2-1965 Fix bug with Setting Tx power of Multi Adv BCM20703A2_001.002.011.0261.0000
BCM20703A2-1962 BLE: support -60dBm Adv Tx power BCM20703A2_001.002.011.0260.0000
BCM20703A2-1960 Multi Adv fixes (equivalent to BLTH03096390 for 4356)
BCM20703A2-1952 - Fix error in FIX_BCM20703A2_1951 BCM20703A2_001.002.011.0257.0000 BCM20703A2_001.002.011.0256.0000
BCM20703A2-1921 - 4354 BRCM PCF: Adv events rcvd only from one adv when filter with two broadcast addresses added on IUT

BCM20703A2-1919 - Fix compiler error BCM20703A2_001.002.011.0244.0000
BCM20703A2-1914 - LE ADV PCF: fix specific filter issue
BCM20703A2-1913 - Add partial Manufacture data filter to LE ADV BRCM PCF
BCM20703A2-1912 - Add partial UUID filter to LE ADV BRCM PCF
BCM20703A2-1910 Add Service Data filter to LE ADV BRCM Packet Content Filter
BCM20703A2-1907 LE ADV BRCM PCA: dynamic filter memory allocation
BCM20703A2-1908 Add missing file from BCM20703A2-1903
BCM20703A2-1893 Fix compilation error with BCM20703A2-1892
BCM20703A2-1883 Key Problems with Native Bluetooth, LMP key validation
BCM20703A2-1892 Patch in Google VSCs Part #1
BCM20703A2-1847 COEX - Defer some COEX init on HCI_ResetBCM20703A2_001.002.011.0231.0000
BCM20703A2-1838 (20706A2) COD overwritten when device in Limited Discovery mode BCM20703A2_001.002.011.0229.0000BCM20703A2_001.002.011.0228.0000
BCM20703A2-1828 LE connection drop during GATT transfer
BCM20703A2-1815 MPAF GPIO driver - workaround LHL GPIO interrupt drop issue
BCM20703A2-1779 [20706A2] save patch entries
BCM20703A2-1789 Multi adv clean up, enable order BCM20703A2_001.002.011.0214.0000
BCM20703A2-1774 Do not invoke lrm_DeleteLink from interrupt context BCM20703A2_001.002.011.0211.0000
BCM20703A2-1760 Remove fix SWWICED-8997 and add only required patches to multiple adv lib BCM20703A2_001.002.011.0207.0000
BCM20703A2-1961 - LE features: support for spec 5.2 (Energy Info VSC support, Multi ADV Tx Power in dBm units)
BCM20703A2-1951 - LE features: Get Controller Debug Info implementation
BCM20703A2-1950 - Features: Add two new Google VSC OCFs in HCI header file according to spec 0.96
BCM20703A2-1949 - LE features: extended scan parameters spec 0.95
BCM20703A2-1928 - Add build target with VSCs BCM20703A2_001.002.011.0246.0000
BCM20703A2-1927 - Batching: integrate existing Batching implementation...
BCM20703A2-1924 - LE Features: Batching FW implementation (except LE Scan / Batch Scan concurrency)
BCM20703A2-1922 - LE features - Energy Info Support
BCM20703A2-1903: Patch in VSCs Part #3 LE_APCF_Command

BCM20703A2-1891 Patch in VSCs Part #2 LE_RPA_offload_Command(0x155)
BCM20703A2-1951 - LE features: Get Controller Debug Info implementation
BCM20703A2-1949 - LE features: extended scan parameters spec 0.95
BCM20703A2-1928 - Add build target with VSCs BCM20703A2_001.002.011.0246.0000
BCM20703A2-1927 - Batching: integrate existing Batching implementation with Adv Filtering
BCM20703A2-1922 - LE features - Energy Info Support
BCM20703A2-1903: Patch in VSCs Part #3 LE_APCF_Command
BCM20703A2-1891 Patch in VSCs Part #2 LE_RPA_offload_Command(0x155)
BCM20703A2-1831 - Key Problems with Native Bluetooth Security
BCM20703A2-2217 - Vulnerability in bcsulp_procRxPayload
BCM20703A2-2164 - Two WBS link support BCM20703A2_001.002.011.0311.0000
BCM20703A2-1957 - - Change the BR/EDR step of WRITE_TX_POWER_TABLE to 1dB BCM20703A2_001.002.011.0259.0000
BCM20703A2-2043- AFH: set the minimum LE channels to be 8
BCM20703A2-2219 - Send connection status to app if connection timeout/failed to establish connection occurs BCM20703A2_001.002.011.0330.0000

VERSION # BCM20703A2_001.002.011.0201.020x

December 2017

The firmware images are built by Cypress to meet Laird Connectivity's requirements and so the version number used utilises the Cypress formats. The firmware is identical between the 2 versions listed below, except for the main host interface being USB or UART respectively.

These were the first mass production released products.

- **BT850 / BT851 - USB**
BCM20703A2_001.002.011.0201.0202
- **BT860 - UART**
BCM20703A2_001.002.011.0201.0203

Further Information

Further information relating to the BT850 / BT851 and BT860 and its firmware is available from the Laird website at

<https://www.lairdconnect.com/bt850-bt851-and-bt860-series-modules-adapter-and-dvks>