BIOS Update Release Notes

PRODUCTS: BC510, BC710

BIOS Version 0082 - BCTGL357.0082.2023.1213.1133

About This Release:

- Date: Dec 13, 2023
- ROM Image Checksum: 0XAB1F62A0
- EC Firmware: 0.39.0.000
- ME Firmware: 15.0.45.2411
- PCH Configuration Firmware: 15.0.0.1021
- PMC Firmware: 150.1.20.1041
- iTBT Firmware: 15.0.0.4801
- IOM Firmware: 17.24.0.0000
- Retimer Firmware in BIOS capsule: 2.13_CCG5_0609_SEC3
- NPHY Firmware: 11.225.276.2043
- CRB Label: 1AWHY_048
- Boot Guard ACM: 1.14.46
- BIOS Guard: BiosGuard_029
- Silicon Initialization Code: 0A.00.5D.32(4303.02)
- Memory Reference Code: 2.0.2.8
- Integrated Graphics:
    - o UEFI Driver: 17.0.1071
- Intel RST Pre-OS:
    - o VMD UEFI Driver: 18.1.1.5201
- AHCI Code: ACHI_24
- Visual BIOS: Intel AptioV

- Supported Flash Devices:

WinBond	W25Q256JV	32MB
GigaDevice	GD25B256D	32MB

- Microcode Updates included in .BIN & .CAP Files:
    - M80806C1_000000B6.pdb

New Fixes/Features/Updates:

- Fixed issue where LogoFAIL vulnerability.
- Updated Secure Boot key.
- Updated NetworkPkg EDK2.
- Fixed issue where “UsbSmmRt” vulnerability.
- Fixed issue where EDK2 PEI-Phase Denial of Service vulnerability.
- Fixed issue where Intel NUC TOCTOU vulnerability.
- Fixed issue where TOCTOU vulnerability in “SmiFlash”.
- Updated CPU Microcode to M80806C1_000000B6.pdb.
- Fixed issue where The values of “iSetupCfg” password check setting cannot be saved when pressing the Save icon in the upper right corner.

Known Errata:

*Other names and brands may be claimed as the property of others.

- Due to a **BC0072** module upgrade, User cannot flash/recover downgrade to BIOS BC0071 or earlier.
- When the BIOS version is below V0051, please update to V0064 first.
- When the BIOS version is between V0064 ~ and V0069, please update to V0071 first.

BIOS Version 0081 - BCTGL357.0081.2023.0809.1704

About This Release:

- Date: August 09, 2023
- ROM Image Checksum: 0XAB24DAF7
- EC Firmware: 0.39.0.000
- ME Firmware: 15.0.45.2411
- PCH Configuration Firmware: 15.0.0.1021
- PMC Firmware: 150.1.20.1041
- iTBT Firmware: 15.0.0.4801
- IOM Firmware: 17.24.0.0000
- Retimer Firmware in BIOS capsule: 2.13_CCG5_0609_SEC3
- NPHY Firmware: 11.225.276.2043
- CRB Label: 1AWHY_048
- Boot Guard ACM: 1.14.46
- BIOS Guard: BiosGuard_029
- Silicon Initialization Code: 0A.00.5D.32(4303.02)
- Memory Reference Code: 2.0.2.8
- Integrated Graphics:
  - UEFI Driver: 17.0.1071
- Intel RST Pre-OS:
  - VMD UEFI Driver: 18.1.1.5201
- AHCI Code: ACHI_24
- Visual BIOS: Intel AptioV

- Supported Flash Devices:

WinBond	W25Q256JV	32MB
GigaDevice	GD25B256D	32MB

- Microcode Updates included in .BIN & .CAP Files:
  - M80806C1_000000AC.pdb

New Fixes/Features/Updates:

- Updated IPU 2023.3 Update.
- Updated Updated BIOS flash tool “iFlashV” to versions 5.13.00.2106 (X64) / 5.13.00.2106 (IA32).
- Updated PlatformLang Timeout Variable Access.
- Updated OpenSSL Policy Constraints.
- Updated BlackLotus-SecureBoot DBX Update.
- Updated Harden SMM Write Flash.
- Fixed issue where Heap Buffer Overflow in TCG2MeasurePeImage.
- Fixed OOB RW vulnerability In select Intel NUC products.
- Updated SmiFlash related solutions including TOCTOU SmiFlash_v2.
- Fixed issue where When the Intel i219 LAN and Thunderbolt support items are Disabled in the BIOS, the system cannot update the BIOS through the Power Button Menu [F7] Flash option.

Known Errata:

- Due to a **BC0072** module upgrade, User cannot flash/recover downgrade to BIOS BC0071 or earlier.
- When the BIOS version is below V0051, please update to V0064 first.
- When the BIOS version is between V0064 ~ and V0069, please update to V0071 first.

BIOS Version 0079 - BCTGL357.0079.2023.0508.1709

About This Release:

- Date: May 08, 2023
- ROM Image Checksum: 0XAB311E91
- EC Firmware: 0.39.0.000
- ME Firmware: 15.0.45.2411
- PCH Configuration Firmware: 15.0.0.1021
- PMC Firmware: 150.1.20.1041
- iTBT Firmware: 15.0.0.4801
- IOM Firmware: 17.24.0.0000
- Retimer Firmware in BIOS capsule: 2.13_CCG5_0609_SEC3
- NPHY Firmware: 11.225.276.2043
- CRB Label: 1AWHY_048
- Boot Guard ACM: 1.14.46
- BIOS Guard: BiosGuard_029
- Silicon Initialization Code: 0A.00.5D.32(4303.02)
- Memory Reference Code: 2.0.2.8
- Integrated Graphics:
  - UEFI Driver: 17.0.1071
- Intel RST Pre-OS:
  - VMD UEFI Driver: 18.1.1.5201
- AHCI Code: ACHI_24
- Visual BIOS: Intel AptioV

- Supported Flash Devices:

WinBond	W25Q256JV	32MB
GigaDevice	GD25B256D	32MB

- Microcode Updates included in .BIN & .CAP Files:
  - M80806C1_000000AC.pdb

New Fixes/Features/Updates:

- Updated IPU 2023.1 Update.
- Fixed issue where UEFI Variable access vulnerability.
- Fixed issue where "SDIO_DEV_CONFIGURATION SetVariable" NVRAM corruption.
- Updated IPU 2023.2 Update.
- Fixed issue where OpenSSL vulnerabilities.
- Updated CPU Microcode updated to M80806C1_000000AC.pdb
- Updated ME FW to 15.0.45.2411

Known Errata:

- Due to a **BC0072** module upgrade, User cannot flash/recover downgrade to BIOS BC0071 or earlier.
- When the BIOS version is below V0051, please update to V0064 first.
- When the BIOS version is between V0064 ~ and V0069, please update to V0071 first.

BIOS Version 0078 - BCTGL357.0078.2023.0103.1344

About This Release:

- Date: 01/03/2023
- ROM Image Checksum: 0XAB5917C8
- EC Firmware: 0.39.0.000
- ME Firmware: 15.0.42.2235
- PCH Configuration Firmware: 15.0.0.1021
- PMC Firmware: 150.1.20.1041
- iTBT Firmware: 15.0.0.4601
- IOM Firmware: 17.23.0.0000
- Retimer Firmware in BIOS capsule: 2.13_CCG5_0609_SEC3
- NPHY Firmware: 11.225.276.20421
- CRB Label: 1AWHY_048
- Boot Guard ACM: 1.14.39
- Bios Guard: BiosGuard_029
- Silicon Initialization Code: 0A.00.5D.32(4303.02)
- Memory Reference Code: 2.0.2.8
- Integrated Graphics:
  - UEFI Driver: 17.0.1071
- Intel RST Pre-OS:
  - VMD UEFI Driver: 18.1.1.5201
- AHCI Code: ACHI_24
- Visual BIOS: Intel AptioV

- Supported Flash Devices:

WinBond	W25Q256JV	32MB
GigaDevice	GD25B256D	32MB

- Microcode Updates included in .BIN & .CAP Files:
  - M80806C1_000000A6.pdb

New Fixes/Features:

- Fixed issue where SmmEntryPoint Underflow Vulnerability.
- Fixed issue where OS Kernel-level malware may cause information disclosure vulnerability.
- Fixed issue where Intel NUC information disclosure vulnerability.
- Fixed issue where GRUB Bootloader Vulnerability.
- Fixed issue where UEFI Boot Variables Access
- Fixed issue where Building Process optimize_avoid UQI duplicated
- Fixed issue where BIOS WU setup added.
- Updated EC Firmware to 0.39.00.000.
- Fixed issue where System fails to warm reset and shutdown when updating IOM FW to 17.23.0.0000.
- Fixed issue where Type-C connect not charging.

- Fixed issue where BIOS Password Entry Points_F8 hot key.

Known Errata:

- Due to a **BC0072** module upgrade, User cannot flash/recover downgrade to BIOS BC0071 or earlier.
- When the BIOS version is below V0051, please update to V0064 first.
- When the BIOS version is between V0064 ~ and V0069, please update to V0071 first.

BIOS Version 0077 - BCTGL357.0077.2022.1004.1426

About This Release:

- Date: 10/04/2022
- ROM Image Checksum: 0xAB5CE1A5
- EC Firmware: 0.38.0.000
- ME Firmware: 15.0.42.2235
- PCH Configuration Firmware: 15.0.0.1021
- PMC Firmware: 150.1.20.1041
- iTBT Firmware: 15.0.0.4601
- IOM Firmware: 17.23.0.0000
- Retimer Firmware in BIOS capsule: 2.13_CCG5_0609_SEC3
- NPHY Firmware: 11.225.276.20421
- CRB Label: 1AWHY_048
- Boot Guard ACM: 1.14.25
- Bios Guard: BiosGuard_029
- Silicon Initialization Code: 0A.00.5D.32(4303.02)
- Memory Reference Code: 2.0.2.8
- Integrated Graphics:
  - UEFI Driver: 17.0.1071
- AHCI Code: ACHI_24
- Visual BIOS: Intel AptioV

- Supported Flash Devices:

WinBond	W25Q256JV	32MB
GigaDevice	GD25B256D	32MB

- Microcode Updates included in .BIN & .CAP Files:
  - M80806C1_000000A6.pdb

New Fixes/Features:

- Updated 2022 IPU CPU Microcode: 2022.1/2022.2/2022.3 M80806C1_000000A6.pdb
- Added Implement S3 reboot code in MS support project.
- Fixed issue where Potential hack of EBU Flash DLL files.
- Fixed issue where SIO_DEV_STATUS_VAR_NAME Information Leakage_PTK2712#12.
- Fixed issue where Intel NUC 8 vulnerability/Intel NUC 8 info leak vulnerability.
- Fixed issue where RSB Stuffing Mitigation for Speculative Execution Vulnerability.
- Fixed issue where UEFI Variable access vulnerability in Intel NUC BIOS.
- Fixed issue where TianoCore Security Issue.

- Updated Modify Wordings in Config Mode.
- Fixed issue where Variable Struct Counter.
- Fixed issue where System cannot get USB working again in BIOS after disabling all the USB ports in the BIOS Setup menu.
- Added StdDefaults into ProtectedNvVariableForRuntime ELink.
- Fixed issue where iSetupCfg not able to change default value of PLx/Fan cuver parameters due to stdDefault override mechanism.
- Fixed issue where Smoke test found that Selftest_138 has 13 errors.
- Fixed issue where System needs more than 30 sec to Boot into Windows.

Known Errata:

- Due to a **BC0072** module upgrade, User cannot flash/recover downgrade to BIOS BC0071 or earlier.
- When the BIOS version is below V0051, please update to V0064 first.
- When the BIOS version is between V0064 ~ and V0069, please update to V0071 first.

BIOS Version 0076 - BCTGL357.0076.2022.0722.1956

About This Release:

- Date: Jul 22, 2022
- ROM Image Checksum: 0xAB82478D
- ME Firmware: Consumer 15.0.35.1898
- EC Firmware: 0.38.00.000
- PMC Firmware: 150.01.20.1039
- Boot Guard ACM: 1.14.25
- Reference Code: Based on 0A.00.5D.32
- Integrated Graphics:
  - UEFI Driver: 17.0.1071
- Visual BIOS: Intel AptioV
- Supported Flash Devices:

WinBond	W25Q256FV	32MB
GigaDevice	GD25B256D	32MB

- Microcode Updates included in .BIN & .CAP Files:
  - M80806C0_0000009a.pdb

New Fixes/Features:

- Updated BootPerformanceTable_pointer.
- Fixed issue where the arbitrary code execution in DXE driver.
- Fixed issue where SMM memory corruption vulnerability in SMM driver on Intel platforms.
- Fixed issue with Stack overflow vulnerability in SMI handler.
- Fixed issue where Privilege escalation vulnerability from kernel to SMM in multiple devices.
- Fixed issue with Intel NUC information leak vulnerability.
- Fixed issue with Information disclosure vulnerability.
- Fixed issue where Arbitrary write vulnerability in PEI module leads to arbitrary code execution in PEI phase.
- Fixed issue where the buffer overflow in UEFI Firmware BIOS core.
- Fixed issue where POST hotkey string display is too long beyond

the screen.
- Fixed issue where LOGITECH Rally Bar produces static noise.
- Fixed issue where Correct EC MMIO Driver (ACPI memory resource RangeLength) to 0x100.
- Added Display a warning message when BIOS upgrade results will mean a BIOS downgrade is no possible. This has been defined in BIOS_Master_RD_v3.10.01.
- Fixed issue where Optimize F6 string layout patch, fix some letters 'y' and 'g' will be truncated by the next line.
- Fixed issue where ME FW minor version checking algorithm.
- Fixed issue where POST hotkey message does not display when Secure Boot is enabled.
- Added Need to report RTC power down status in OemCheckRtcLostPower function.
- Fixed issue where fTPM does not function after RTC lost power.

Known Errata:
- Due to a **BC0072** module upgrade, User cannot flash/recover downgrade to BIOS BC0071 or earlier.
- When the BIOS version is below V0051, please update to V0064 first.
- When the BIOS version is between V0064 ~ and V0069, please update to V0071 first.

BIOS Version 0075 - BCTGL357.0075.2022.0513.1246

About This Release:
- Date: May 13, 2022
- ROM Image Checksum: 0xAB85C5CB
- ME Firmware: Consumer 15.0.35.1898
- EC Firmware: 0.38.00.000
- PMC Firmware: 150.01.20.1039
- Boot Guard ACM: 1.14.25
- Reference Code: Based on 0A.00.5D.32
- Integrated Graphics:
  - UEFI Driver: 17.0.1071
- Visual BIOS: Intel AptioV

- Supported Flash Devices:

WinBond	W25Q256FV	32MB
GigaDevice	GD25B256D	32MB

- Microcode Updates included in .BIN & .CAP Files:
  - M80806C0_0000009a.pdb

New Fixes/Features:
- Updated BIOS code for security fixes.
- Updated EC Firmware to 0.38.00.000.
- Fixed HP monitor/laptop power issue.
- Fixed issue that did not allow the use of the tool to do EC update in EFI Shell.
- Fixed issue with BIOS Warning message during BIOS Windows Update.
- Fixed issue with Watchdog Timer that did not restart system under

Ubuntu 20.04(LTS).

- Fixed issue when updating to BIOS BC0072, after the update progress reached 100%, the units hung up, did not reboot.
- Updated PD Firmware to v6.1F. Fixes support for Power Delivery when using an HP monitor with Type-C that won't power the laptop.

BIOS Version 0074 - BCTGL357.0074.2022.0331.2129

About This Release:

- Date: Mar 31, 2022
- ROM Image Checksum: 0xAB8C25F5
- ME Firmware: Consumer 15.0.35.1898
- EC Firmware: 0.36.00.000
- PMC Firmware: 150.01.20.1039
- Boot Guard ACM: 1.14.25
- Reference Code: Based on 0A.00.5D.32
- Integrated Graphics:
  - UEFI Driver: 17.0.1071
- Visual BIOS: Intel AptioV
- Supported Flash Devices:
  - WinBond W25Q256FV 32MB
  - GigaDevice GD25B256D 32MB
- Microcode Updates included in .BIN & .CAP Files:
  - M80806C0_0000009a.pdb

New Fixes/Features:

- Updated Config Mode Default Setting.
- Fixed issue where could not clear Event Log using the command: **AfuMfgWINx64.EXE PAxx.CAP /oemsmi:ac /cmd:{CELOG}**

BIOS Version 0072 - BCTGL357.0072.2022.0118.1440

About This Release:

- Date: Jan 18, 2022
- ROM Image Checksum: 0xAB6CF1A3
- ME Firmware: Consumer 15.0.35.1898
- EC Firmware: 0.35.00.000
- PMC Firmware: 150.01.20.1039
- Boot Guard ACM: 1.14.25
- Reference Code: Based on 0A.00.5D.32
- Integrated Graphics:
  - UEFI Driver: 17.0.1071
- Visual BIOS: Intel AptioV
- Supported Flash Devices:
  - WinBond W25Q256FV 32MB
  - GigaDevice GD25B256D 32MB
- Microcode Updates included in .BIN & .CAP Files:
  - M80806C0_0000009A.pdb

New Fixes/Features:

- Updated CPU Microcode 09A for 2021.2 IPU BIOS change.
- Changed Bluetooth Audio Offload on Windows 11.
- Updated EC version to 0.35.00.000.

*Other names and brands may be claimed as the property of others.

- Fixed issue with Hardware Security Testability Interface Test (0x00110001 - RollBack Firmware Error).
- Fixed Windows 11 HLK HSTI: Unexpected Status 0x00080003 Platform Security Specification - Memory Map Security Configuration - Non lockable MMIO ranges overlap other critical regions.
- Fixed ACPI BIOS error after installing NPSS into Ubuntu.
- Fixed issue with Bluetooth - Initiate platform-level device reset Fail.
- Fixed issue where Realtek audio driver could not install after update to CRB044.
- Added customization option of integrated Numpad (Fn hotkey).
- Fixed issuew where unauthorized modification of UEFI variables could disable the protect mechanism of SMM.
- Fixed issue that could not find recovery file in NVME.
- Added disable NVRAM update and reserve RC setup variables.
- Fixed issue with progress bar update display.
- Updated GOP to 17.0.1071 for Windows 11 support.
- Fixed issue that could not exit BIOS Setup when pressing exit button.
- Fixed system hang issue on "F7" flash page (Remove or reinsert USB key).
- Fixed issue where D20/F2 SVID/SSID were not set.
- Updated ME Firmware to version 15.0.35.1898 v3 for Windows 11 support.
- Fixed BIOS setup issue where "Intel Platform Trust Technology" item disappeared.
- Fixed issue that could not capsule update after updating to CRB048.
- Fixed issue where PXE Boot failed to show WDS Boot Manager screen.
- Fixed issue with read recovery file on Type-C port.
- Updated to CRB048 code.

Known Errata:

- Due to a **BC0072** module upgrade, User cannot flash/recover downgrade to BIOS BC0071 or earlier.

BIOS Version 0071 - BCTGL357.0071.2021.1021.1647

About This Release:

- Date: Oct 21, 2021
- ROM Image Checksum: 0xA98A796B
- ME Firmware: Consumer 15.0.23.1706
- EC Firmware: 0.34.00.000
- PMC Firmware: 150.01.20.1035
- Boot Guard ACM: 1.14.15
- Reference Code: Based on 0A.00.3C.21
- Integrated Graphics:
  - UEFI Driver: 17.0.1055
- Visual BIOS: Intel AptioV
- Supported Flash Devices:
  - WinBond W25Q256FV 32MB
  - GigaDevice GD25B256D 32MB
- Microcode Updates included in .BIN & .CAP Files:

*Other names and brands may be claimed as the property of others.

    - M80806C0_00000068.pdb
    - M80806C1_00000086.pdb

New Fixes/Features:

- Fixed missing "Intel Platform Trust Technology" item in BIOS setup.
- Updated EC version to 0.34.00.000
- Fixed issue with PXE Boot that failed to show WDS Boot Manager screen.
- Fixed issue where could not read Recovery CAP file when using Type-C port.
- Added NvramReflash module that solved the problem of unreserved RC setup variables.
- Fixed issue with Microsoft OA3 Tool.

Known Errata:

- Due to a BC0071 module upgrade, User cannot flash/recover downgrade to BIOS BC0069 or earlier.
- BC0071 enables an NVRAM update. When the onboard BIOS is BC0071, during the capsule update progress, 0%~20% is the BIOS code update. 21%~100% is NVRAM update.
  Fault tolerance will fail if unplugging both Adapter and Battery from the system during the BIOS update process to 21%~100%.

BIOS Version 0069 - BCTGL357.0069.2021.0806.2223

About This Release:

- Date: Aug 06, 2021
- ROM Image Checksum: 0xA990FFE4
- ME Firmware: Consumer 15.0.23.1706
- EC Firmware: 0.33.00.000
- PMC Firmware: 150.01.20.1035
- Boot Guard ACM: 1.14.15
- Reference Code: Based on 0A.00.3C.21
- Integrated Graphics:
    - UEFI Driver: 17.0.1055
- Visual BIOS: Intel AptioV

- Supported Flash Devices:
    - WinBond   W25Q256FV   32MB
    - GigaDevice GD25B256D   32MB

- Microcode Updates included in .BIN & .CAP Files:
    - M80806C0_00000068.pdb
    - M80806C1_00000086.pdb

New Fixes/Features:

- Updated BIOS code for security fixes.
- Fixed lag noticed with mouse when using Bluetooth connectivity.
- Disabled Time Of Flight (TOF) according to non-touch panel feature.

BIOS Version 0067 - BCTGL357.0067.2021.0713.2249

About This Release:

- Date: Jul 13, 2021
- ROM Image Checksum: 0xA9E7CF6B
- ME Firmware: Consumer 15.0.23.1706
- EC Firmware: 0.33.00.000
- PMC Firmware: 150.01.20.1035
- Boot Guard ACM: 1.14.15
- Reference Code: Based on 0A.00.3C.21
- Integrated Graphics:
  - Option ROM: N/A
  - UEFI Driver: 17.0.1055
- Visual BIOS: Intel AptioV
- Supported Flash Devices:
  - WinBond W25Q256FV 32MB
  - GigaDevice GD25B256D 32MB
- Microcode Updates included in .BIN & .CAP Files:
  - M80806C0_00000068.pdb
  - M80806C1_00000086.pdb

New Fixes/Features:

- Updated: ME FW version to 15.0.23.1706 v3.

BIOS Version 0064 - BCTGL357.0064.2021.0518.1820

About This Release:

- Date: May 18, 2021
- ROM Image Checksum: 0xA869DCCB
- ME Firmware: Consumer 15.0.10.1447 (ROM burner)
- ME Firmware: Consumer 15.0.10.1377 (Capsule update from BC0051/54/57/61)
- EC Firmware: 0.32.00
- PMC Firmware: 150.01.20.1028
- Boot Guard ACM: 1.14.15
- Reference Code: Based on 0A.00.3C.21
- Integrated Graphics:
  - UEFI Driver: 17.0.1045
- Visual BIOS: Intel AptioV
- Supported Flash Devices:
  - WinBond W25Q256FV 32MB
  - GigaDevice GD25B256D 32MB
- Microcode Updates included in .BIN & .CAP Files:
  - M80806C0_00000068.pdb
  - M80806C1_00000078.pdb
  - M80806D0_0000004C.pdb

New Fixes/Features:

- Fix issue when pressing “fn + num-lock” did not switch to the enabled state.
- Fix issue with LCD brightness which dimmed during warm boot process.

BIOS Version 0060 - BCTGL357.0060.2021.0324.1856

About This Release:

- Date: Mar 24, 2021
- ROM Image Checksum: 0xA95F51B1

- ME Firmware: Consumer 15.0.10.1447
- EC Firmware: 0.31.00
- PMC Firmware: 150.01.20.1028
- Boot Guard ACM: 1.14.15
- Reference Code: Based on 0A.00.3C.21
- Integrated Graphics:
  - Option ROM: N/A
  - UEFI Driver: 17.0.1045
- Intel RST Pre-OS:
  - Option ROM: N/A
  - RAID Option ROM: N/A
- Supported Flash Devices:
  - WinBond W25Q256FV 32MB
  - GigaDevice GD25B256D 32MB
- Microcode Updates included in .BIN & .CAP Files:
  - M80806C0_00000068.pdb
  - M80806C1_00000068.pdb
  - M80806D0_0000004C.pdb

New Fixes/Features:

- Replaced power button menu with security jumper menu in configuration mode.
- Added WLAN disabling feature in Setup, boot to OS, BT is also disabled.
- Updated Retimer Firmware version.
- Added new LAN PXE boot support feature in USB/LAN dongle AX88179 and RTL8152/RTL8153.
- Fixed keyboard FN lock reset after reboot.
- Fixed issues with OFBD module SMI handler.
- Fixed issue with NTFS DXE driver in process of parsing NTFS file system partition.

BIOS Version 0057 - BCTGL357.0057.2021.0203.1856

About This Release:

- Date: Feb 3, 2021
  - ROM Image Checksum: 0xAEF54B6A
- ME Firmware: Consumer 15.0.2.1377
- EC Firmware: 0.31.00
- PMC Firmware: 150.01.20.1024
- Boot Guard ACM: 1.14.8
- Reference Code: Based on 0A.00.2A.30
- Integrated Graphics:
  - Option ROM: N/A
  - UEFI Driver: 17.0.1044
- Visual BIOS: Intel Aptio V
- Supported Flash Devices:
  - WinBond W25Q256FV 32MB
  - GigaDevice GD25B256D 32MB
- Microcode Updates included in .BIN & .CAP Files:
  - M80806C0_00000068.pdb
  - M80806C1_00000060.pdb
  - M80806D0_00000030.pdb

New Fixes/Features:

- Updated: EC FW version to 0.31.00.000.
- Fixed: Where you could not boot into BIOS recovery when using a LG 5K Monitor.
- Fixed: Using F7 to update will update the BIOS will also update the ME firmware.
- Fixed: Virtual Number pad that was non-functional.
- Added: Deep S4/S5 option to Setup menu.
- Fixed: iGFX SSID.
- Added: New battery information shown in ESA BIOS setup.

BIOS Version 0051 - BCTGL357.0051.2020.1207.1547

About This Release:

- Date: Dec 8, 2020
- ROM Image Checksum: 0xACB7574B
- ME Firmware: Consumer 15.0.2.1377
- EC Firmware: 0.28.00
- PMC Firmware: 150.01.20.1024
- Boot Guard ACM: 1.14.8
- Reference Code: Based on 0A.00.2A.30
- Integrated Graphics:
  - Option ROM: N/A
  - UEFI Driver: 17.0.1044
- Visual BIOS: Intel AptioV

- Supported Flash Devices:
  - WinBond   W25Q256FV   32MB
  - GigaDevice GD25B256D   32MB

- Microcode Updates included in .BIN & .CAP Files:
  - M80806C0_00000068.pdb
  - M80806C1_00000060.pdb
  - M80806D0_00000030.pdb

New Fixes/Features:

- Fixed Issue: Touch panel ghost point during LID open / LID close
- Functionality Updates

BIOS Version 0048 - BCTGL357.0048.2020.1118.2111

About This Release:

- Date: Nov 18, 2020
- ROM Image Checksum: 0xAE1E7966
- ME Firmware: Consumer 15.0.2.1377
- EC Firmware: 0.28.00
- PMC Firmware: 150.01.20.1024
- Boot Guard ACM: 1.14.8
- Reference Code: Based on 0A.00.2A.30
- Integrated Graphics:
  - Option ROM: N/A
  - UEFI Driver: 17.0.1044
- Intel RST Pre-OS:
  - Option ROM: N/A
  - RAID Option ROM: N/A

- Supported Flash Devices:

WinBond	W25Q256FV	32MB
GigaDevice	GD25B256D	32MB

- Microcode Updates included in .BIN & .CAP Files:
  - M80806C0_00000068.pdb
  - M80806C1_00000060.pdb
  - M80806D0_00000030.pdb

New Fixes/Features:

- Initial production BIOS release

LEGAL INFORMATION

Information in this document is provided in connection with Intel Products and for the purpose of supporting Intel developed server/desktop boards and systems.

No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted by this document. Except as provided in Intel's Terms and Conditions of Sale for such products, Intel assumes no liability whatsoever, and Intel disclaims any express or implied warranty, relating to sale and/or use of Intel products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right. Intel Corporation may have patents or pending patent applications, trademarks, copyrights, or other intellectual property rights that relate to the presented subject matter. The furnishing of documents and other materials and information does not provide any license, express or implied, by estoppel or otherwise, to any such patents, trademarks, copyrights, or other intellectual property rights. Intel products are not intended for use in medical, life saving, or life sustaining applications. Intel may make changes to specifications and product descriptions at any time, without notice.

Intel is a trademark of Intel Corporation in the US and other countries.