BIOS Update Release Notes

PRODUCTS: CM11EBV58W, CM11EBV716W

BIOS Version 0061 - EBTGLMIV.0061.2021.0702.1647

About This Release:

- Date: July 2, 2021
- ROM Image Checksum: 0xF86D
- ME Firmware: Corporate 15.0.22.1680
- EC1 Firmware:
  - AB_A: 2.23.0
  - AB_B: 2.23.0
  - AB_C: 2.23.1
  - BB: 2.21.0
  - Test Board: 2.16.0
  - FB: 2.24.0
  - EB Test Board: 3.1.0_1.16r11
  - CC: 3.2.11_1.17_r25_OEM_0.0.2_PD_260300002120_8233_010205_PDT_201217
  - GB: 2.6.0_v1.17_r11_PD_241100002020
- EC2 Firmware: 2.17.0
- PMC Firmware: 150.01.20.1033
- Boot Guard ACM: 1.14.10
- Memory Reference Code: 1.0.12.0
- MEBx Revision: 15.0.0.0003
- Integrated Graphics:
  - UEFI Driver: 17.0.1059
- Intel RST VMD Pre-OS:
  - UEFI Driver: 18.1.1.5201
- AHCI Code: Based on AHCI_24
- Visual BIOS: Intel AptioV Text Setup

- Supported Flash Devices:
  - WinBond W25Q256JV 32MB
  - GigaDevice GD25B256D 32MB
  - Macronix MX77L25650F 32MB

- Microcode Updates included in .BIN & .CAP Files:
  - m_80_806c1_0000007e.pdb

New Fixes/Features:

- Update needed for audio driver package.
- Updated EC1 Firmware.
- Updated help string of setup "FnLock" item.
- Enable Bluetooth Audio Offload related setup items.
- Updated eDP related setup items.
- Fixed issue with power item due to incorrect behavior.
- Removed non-supported SMBIOS type from CB/EB.
- Updated iFlashV tool "/jbc" command support.
- Allowed for "Failsafe Watchdog" setup option.

- Implemented "BiosGuard" solution for PEI buffer overflow.

Errata:

- To include Realtek Hash into this BIOS, you would need to do a recovery update instead of a normal flash update.

BIOS Version 0056 - EBTGLMIV.0056.2021.0507.1806

About This Release:

- Date: May 7, 2021
- ROM Image Checksum: 0x0382
- ME Firmware: Corporate 15.0.22.1680
- EC1 Firmware:
  - AB_A: 2.23.0
  - AB_B: 2.23.0
  - AB_C: 2.23.0
  - BB: 2.21.0
  - Test Board: 2.16.0
  - FB: 2.24.0
  - EB Test Board: 3.1.0_1.16r11
  - CC: 3.2.0_1.17_r23_OEM_0.0.2_PD_240200002120_8233_010205_PDT_201217
  - GB: 2.5.0_v1.17r10
- EC2 Firmware: 2.17.0
- PMC Firmware: 150.01.20.1033
- Boot Guard ACM: 1.14.10
- Memory Reference Code: 1.0.12.0
- MEBx Revision: 15.0.0.0003
- Integrated Graphics:
  - UEFI Driver: 17.0.1059
- Intel RST VMD Pre-OS:
  - UEFI Driver: 18.1.1.5201
- AHCI Code: Based on AHCI_24
- Visual BIOS: Intel Text Setup

- Supported Flash Devices:
  - WinBond W25Q256JV 32MB
  - GigaDevice GD25B256D 32MB
  - Macronix MX77L25650F 32MB

- Microcode Updates included in .BIN & .CAP Files:
  - m_80_806c1_0000007e.pdb

New Fixes/Features:

- Fixed issue with Bluetooth device yellow mark after S4 resume.
- Fixed Security Jumper Display string.
- Updated PCH ChipsetInit Firmware.
- Updated CPU Microcode to version 0x7e.
- Enabled token "BEEP_ENABLE" to make sound.
- Corrected the battery information data and battery mode string behavior.
- Added ability to achieve arbitrary write in SMRAM save state region.

- Updated ME Firmware to 15.0.22.1680.
- Updated AB/BB/FB EC Firmware.
- Updated CC carrier EC Firmware to 3.2.0_1.17.
- Updated OemModulePkg.
- Fixed OFBD module SMI handler vulnerabilities.
- Corrected the string shown on exiting config mode.
- Fixed issue while taking pictures with internal webcam did not show mirror image.
- Updated NTFS DXE driver when parsing NTFS file system partition.

BIOS Version 0049 - EBTGLMIV.0049.2021.0226.2146

About This Release:

- Date: February 26, 2021
- ROM Image Checksum: 0x92F2
- ME Firmware: Corporate 15.0.10.1447
- EC1 Firmware:
    - AB_A: 2.21.0
    - AB_B: 2.21.0
    - AB_C: 2.21.0
    - BB: 2.19.0
    - Test Board: 2.16.0
    - FB: 2.22.0
    - EB Test Board: 3.1.0_1.16r11
    - CC: 3.0.16_1.17_r19_OEM_0.0.1_PD_190100002120_8233_010203
    - GB: 2.5.0_v1.17r10
- EC2 Firmware: 2.15.0
- PMC Firmware: 150.01.20.1028
- Boot Guard ACM: 1.14.10
- Memory Reference Code: 1.0.10.0
- MEBx Revision: 15.0.0.0003
- Integrated Graphics:
    - UEFI Driver: 17.0.1052
- Intel RST VMD Pre-OS:
    - UEFI Driver: 18.1.1.5201
- AHCI Code: Based on AHCI_24
- Visual BIOS: Intel Text Setup

- Supported Flash Devices:
    - WinBond W25Q256JV 32MB
    - GigaDevice GD25B256D 32MB
    - Macronix MX77L25650F 32MB

- Microcode Updates included in .BIN & .CAP Files:
    - m_80_806c1_00000072.pdb

New Fixes/Features:

- Updated battery information in BIOS setup.
- Updated Trusted Product Module Firmware.
- Updated Retimer Firmware to rev. 1.7.

- Fixed issue with Unique ID (UUID) that could not be updated under certain conditions.
- Updated ME Firmware Interface Table (FIT) setting.
- Updated GB EC Firmware.
- Fixed issue where a WatchDog event was triggered after persistent mode was enabled.

BIOS Version 0045 - EBTGLMIV.0045.2021.0118.1833

About This Release:

- Date: January 18, 2021
- ROM Image Checksum: 0x44C7
- ME Firmware: Corporate 15.0.10.1447
- EC1 Firmware:
    - AB_A: 2.20.0
    - AB_B: 2.20.0
    - AB_C: 2.20.0
    - BB: 2.18.0
    - Test Board: 2.16.0
    - FB: 2.20.0
    - EB Test Board: 3.1.0_1.16r11
    - CC: 3.0.13_1.17_r18_OEM_0.0.1_PD_131100002020_8233_010202
    - GB: 2.3.0_v1.16r9
- EC2 Firmware: 2.15.0
- PMC Firmware: 150.01.20.1028
- Boot Guard ACM: 1.14.10
- Memory Reference Code: 1.0.10.0
- MEBx Revision: 15.0.0.0003
- Integrated Graphics:
    - UEFI Driver: 17.0.1052
- Intel RST VMD Pre-OS:
    - UEFI Driver: 18.1.1.5201
- AHCI Code: Based on AHCI_24
- Visual BIOS: Intel Text Setup

- Supported Flash Devices:
    - WinBond W25Q256JV 32MB
    - GigaDevice GD25B256D 32MB
    - Macronix MX77L25650F 32MB

- Microcode Updates included in .BIN & .CAP Files:
    - m_80_806c1_00000072.pdb

New Fixes/Features:

- Fixed issues with “F7” BIOS update failure, delays in reboot time and unexpected system shutdowns.

BIOS Version 0036 - EBTGLMIV.0036.2020.1124.2027

About This Release:

- Date: November 24, 2020
- ROM Image Checksum: 0x52F5
- ME Firmware: Corporate 15.0.10.1447

- EC1 Firmware:
    - AB_A: 2.20.0
    - AB_B: 2.20.0
    - AB_C: 2.20.0
    - BB: 2.18.0
    - Test Board: 2.16.0
    - FB: 2.20.0
    - EB Test Board: 2.3.0_1.16r9
    - CC: 2.1.3_1.16_r13_v0.7_v1.2.2_03112020
    - GB: 2.1.0_v1.16r7
- EC2 Firmware: 2.15.0
- PMC Firmware: 150.01.20.1028
- Boot Guard ACM: 1.14.10
- Memory Reference Code: 1.0.10.0
- MEBx Revision: 15.0.0.0003
- Integrated Graphics:
    - UEFI Driver: 17.0.1045
- Intel RST VMD Pre-OS:
    - UEFI Driver: 18.0.3.5032
- AHCI Code: Based on AHCI_24
- Visual BIOS: Intel Text Setup

- Supported Flash Devices:
    - WinBond W25Q256JV 32MB
    - GigaDevice GD25B256D 32MB

- Microcode Updates included in .BIN & .CAP Files:
    - m_80_806c1_0000006C.pdb

New Fixes/Features:

- Initial production BIOS release

LEGAL INFORMATION