BIOS Update Release Notes

PRODUCTS: NUC11TNBv5/K/H, NUC11TNBv7/K/H

BIOS Version 0058 – TNTGLV57.0058.2021.0813.1731

About This Release:

- Date: Aug 13, 2021
- ROM Image Checksum: 44751178
- ME Firmware: 15.0.10.1574v1.2
- EC Firmware: TIGA370000
- PMC Firmware: PMC_B0_150.01.20.1032_prod
- Boot Guard ACM: 1.14.15
- Memory Reference Code: Based on 0A.00.30.51
- Integrated Graphics:
  - UEFI Driver: 17.0.1052
- Intel RST Pre-OS:
  - VMD UEFI Driver: 18.0.5.5115
- AHCI Code: Based on AHCI_24
- Wired LAN Adapter:
  - UEFI Driver: 0.8.05
- Visual BIOS: Intel AptioV

- Supported Flash Devices:
  - MACRONIX MX25L25645G 32MB

- Microcode Updates included in .BIN & .CAP Files:
  - m80806c1_0000008a
  - m80806c1_0000007e

New Fixes/Features:

- Fixed EC Firmware text typo during BIOS flash update.
- Updated CPU Microcode to m80806c1_0000008a, m80806c1_0000007e.
- Updated ME Firmware to 15.0.10.1574v1.2
- Added event log support for Auto RTC feature.
- Fixed issue where Virtual Display emulation did not allow BIOS KVM access.
- Added: [EIP618160] Put the PCON FW Update FMP driver into the BIOS region.
- Added pop-up warning message to user when transition BIOS is necessary.
- Added new BIOS item: Force-enable power to 2242 m.2 slot.

Known Errata:

- Flashing from TNv0052/TNv0053 to TNv0054 still stay on POST logo for about 4mins, TNv0054 to TNv0054 will not see this.
- TNv0032 added code change for new DmiEdit tool, please use latest version of AMI/Intel tools.

BIOS Version 0057 – TNTGLV57.0057.2021.0609.1511

About This Release:

- Date: Jun, 9 2021
- ROM Image Checksum:
- ME Firmware: 15.0.10.1469
- EC Firmware: TIGA36.00.00
- PMC Firmware: 150.01.20.1028
- Boot Guard ACM: 1.14.15
- Memory Reference Code: Based on 0A.00.30.51
- Integrated Graphics:
  - UEFI Driver: 17.0.1052
- Intel RST Pre-OS:
  - VMD UEFI Driver: 18.0.5.5115
- AHCI Code: Based on AHCI_24
- Wired LAN Adapter:
  - UEFI Driver: 0.8.05
- Visual BIOS: Intel AptioV

- Supported Flash Devices:
  - MACRONIX MX25L25645G 32MB

- Microcode Updates included in .BIN & .CAP Files:
  - M80806C1_00000072.pdb

New Fixes/Features:

- Disabled BIOS Manufacturing mode.

BIOS Version 0056 - TNTGLV57.0056.2021.0513.1633

About This Release:

- Date: May, 13 2021
- ROM Image Checksum: 3f128e6f
- ME Firmware: 15.0.10.1469
- EC Firmware: TIGA360000
- PMC Firmware: 150.01.20.1028
- Boot Guard ACM: 1.14.15
- Memory Reference Code: Based on 0A.00.30.51
- Integrated Graphics:
  - UEFI Driver: 17.0.1052
- Intel RST Pre-OS:
  - VMD UEFI Driver: 18.0.5.5115
- AHCI Code: Based on AHCI_24
- Wired LAN Adapter:
  - UEFI Driver: 0.8.05
- Visual BIOS: Intel AptioV

- Supported Flash Devices:
  - MACRONIX MX25L25645G 32MB

- Microcode Updates included in .BIN & .CAP Files:
  - M80806C1_00000072.pdb

New Fixes/Features:

- Fixed issue where help text was missing after loading “F9” defaults.
- Updated EC Firmware to TIGA360000.
- Fixed issue where after re-plugging HDMI/Type-C cable on the boot

menu screen, the screen was abnormal.
- Fixed issue when Fan control mode was set to “Custom”, CPU fan was not spinning.

BIOS Version 0054 - TNTGLV57.0054.2021.0316.1434

About This Release:

- Date: Mar, 16 2021
- ROM Image Checksum: de091b25
- ME Firmware: 15.0.10.1469
- EC Firmware: TIGA340000
- PMC Firmware: 150.01.20.1028
- Boot Guard ACM: 1.14.15
- Memory Reference Code: Based on 0A.00.30.51
- Integrated Graphics:
  - UEFI Driver: 17.0.1052
- Intel RST Pre-OS:
  - VMD UEFI Driver: 18.0.5.5115
- AHCI Code: Based on AHCI_24
- Wired LAN Adapter:
  - UEFI Driver: 0.8.05
- Visual BIOS: Intel AptioV

- Supported Flash Devices:
  - MACRONIX MX25L25645G 32MB

- Microcode Updates included in .BIN & .CAP Files:
  - M80806C1_00000072.pdb

New Fixes/Features:

- Fixed POST display emulation after HDMI reconnection.
- Updated Retimer dynamic function.
- Updated EC firmware to TIGA340000
- Updated ME firmware to 15.0.10.1469
- Updated Retimer firmware to 2.17
- Changed virtual display setup.
- Fixed ME upgrade failure using security jumper recovery.
- Updated TXT version to 1.14.15
- Fixed issue with USB2.0 port functionality after disabling Thunderbolt™ Support in the BIOS.
- Changed Cooling-Balanced Fan Off Temperature of CPUVR default.
- Enabled "TCO Timer" setup option.
- Adjusted POST screen QRCode position.
- Added Self-Healing module.
- Updated CPU Microcode to m80806c1_00000072.
- Configured Secure Erase mode to Real mode for vPro.
- Fixed issue where system would stay on POST logo screen for about 4 minutes before flash update started.
- Updated NTFS DXE driver regarding parsing NTFS file system partition.
- Fixed issue with display emulation missing POST information after HDMI re-plug in.

BIOS Version 0042 – TNTGLV57.0042.2020.1221.1758

About This Release:

- Date: Dec 22, 2020
- ROM Image Checksum: 13aaaa03
- ME Firmware: 15.0.10.1447
- EC Firmware: TIGA320000
- PMC Firmware: 150.01.20.1028
- Boot Guard ACM: 1.14.12
- Memory Reference Code: Based on 0A.00.30.51
- Integrated Graphics:
  - UEFI Driver: 17.0.1045
- Intel RST Pre-OS:
  - VMD UEFI Driver: 18.0.2.5008
- AHCI Code: Based on AHCI_24
- Wired LAN Adapter:
  - UEFI Driver: 0.8.05
- Visual BIOS: Intel AptioV

- Supported Flash Devices:
  - MACRONIX MX25L25645G 32MB

- Microcode Updates included in .BIN & .CAP Files:
  - M80806C1_0000006C.pdb

New Fixes/Features:

- Initial production BIOS release