BIOS Update Release Notes

PRODUCTS: DE3815TYKHE, DE3815TYBE (Standard BIOS)

NOTE:
This BIOS update is for Intel® NUC Kit DE3815TYHE with the following SA numbers: H27002-400, -401, -402, -404, and -404 and for Intel® NUC Board DE3815TYBE with the following AA numbers: H26998-401, -402, -403, -404, and -405.

BIOS Version 0067 - TYBYT10H.86A.0067.2019.0812.1101

About This Release:

- Date: August 12, 2019
- ROM Image Checksum: 0xF140
- ME Firmware: 1.0.2.1067
- Memory Reference Code: Based on 1.5.0
- Integrated Graphics:
  - Option ROM: 36.2.5 Build 3757
  - UEFI Driver: 7.2.1008
- AHCI Code: Based on 5.004_AHCI_02
- LAN Option ROM: 2.59
- Visual BIOS: 2.2.20
- Supported Flash Devices:

Macronix	MX25U6435FM2I-10G	8MB
Winbond	W25Q64FWSSIG	8MB

- Microcode Updates included in .ROM & .BIO Files:
  - M0C30673321.PDB
  - M0C30678829.PDB
  - M0130673326.PDB
  - M0130679902.PDB

New Fixes/Features:

- Updated BIOS code for security fixes.

BIOS Version 0066 - TYBYT10H.86A.0066.2019.0704.1818

About This Release:

- Date: July 4, 2019
- ROM Image Checksum: 0x478E
- ME Firmware: 1.0.2.1067
- Memory Reference Code: Based on 1.5.0
- Integrated Graphics
  - Option ROM: 36.2.5 Build 3757
  - UEFI Driver: 7.2.1008
- AHCI Code: Based on 5.004_AHCI_02
- LAN Option ROM: 2.59
- Visual BIOS: 2.2.20
- Supported Flash Devices:

Macronix	MX25U6435FM2I-10G	8MB
Winbond	W25Q64FWSSIG	8MB

- Microcode Updates included in .ROM File:
  M0C30673321.PDB
  M0C30678829.PDB
  M0130673326.PDB
  M0130679902.PDB
- Additional Microcode Updates included only in .BIO File:
  M0C30673321.PDB
  M0C30678829.PDB
  M0130673326.PDB
  M0130679902.PDB

New Fixes/Features:

- Updated BIOS code for security fixes.

BIOS Version 0065 - TYBYT10H.86A.0065.2019.0318.1153

About This Release:

- Date: March 18, 2019
- ME Firmware: 1.0.2.1067
- Memory Reference Code: Based on 1.5.0
- Integrated Graphics
  - Option ROM: 36.2.5 Build 3757
  - UEFI Driver: 7.2.1008
- AHCI Code: Based on 5.004_AHCI_02
- LAN Option ROM: 2.59
- Visual BIOS: 2.2.20

New Fixes/Features:

- Updated BIOS code for security fixes.

BIOS Version 0064 - TYBYT10H.86A.0064.2018.0531.1547

About This Release:

- Date: May 31, 2018
- ME Firmware: 1.0.2.1067
- Memory Reference Code: Based on 1.5.0
- Integrated Graphics
  - Option ROM: 36.2.5 Build 3757
  - UEFI Driver: 7.2.1008
- AHCI Code: Based on 5.004_AHCI_02
- LAN Option ROM: 2.59
- Visual BIOS: 2.2.20

New Fixes/Features:

- Security enhancements.

BIOS Version 0063 - TYBYT10H.86A.0063.2018.0226.1511

About This Release:

- Date: February 26, 2018
- ME Firmware: 1.0.2.1067
- Memory Reference Code: Based on 1.5.0
- Integrated Graphics
  - Option ROM: 36.2.5 Build 3757
  - UEFI Driver: 7.2.1008

- AHCI Code: Based on 5.004_AHCI_02
- LAN Option ROM: 2.59
- Visual BIOS: 2.2.20

New Fixes/Features:

- Updated CPU Microcode (Security Advisory-00088)

BIOS Version 0062 - TYBYT10H.86A.0062.2018.0109.1037

About This Release:

- Date: January 9, 2018
- ME Firmware: 1.0.2.1067
- Memory Reference Code: Based on 1.5.0
- Integrated Graphics:
  - Option ROM: 36.2.5 Build 3757
  - UEFI Driver: 7.2.1008
- AHCI Code: Based on 5.004_AHCI_02
- LAN Option ROM: 2.59
- Visual BIOS: 2.2.20

New Fixes/Features:

- Fixed issue where SMBIOS information wasn't displayed correctly using WMI.

BOIS Version 0061 - TYBYT10H.86A.0061.2017.1011.1904

About This Release:

- Date: October 11, 2017
- ME Firmware: 1.0.2.1067
- Memory Reference Code: Based on 1.5.0
- Integrated Graphics
  - Option ROM: 36.2.5 Build 3757
  - UEFI Driver: 7.2.1008
- AHCI Code: Based on 5.004_AHCI_02
- LAN Option ROM: 2.59
- Visual BIOS: 2.2.20

New Fixes/Features:

- Add the setup option "Allow UEFI Third Party Driver loaded".
- Set BIOS lock always enabled per Issue#317952 BIOS write protect.
- Added Flash SMI support.
- Due to a security enhancement, it will not be possible to go to any BIOS earlier than BIOS 0061.
- Added BIOS protection for security enhancement.

BIOS Version 0060 - TYBYT10H.86A.0060.2017.0517.1042

About This Release:

- Date: May 17, 2017
- ME Firmware: 1.0.2.1067
- Memory Reference Code: Based on 1.5.0
- Integrated Graphics
  - Option ROM: 36.2.5 Build 3757
  - UEFI Driver: 7.2.1008

- AHCI Code: Based on 5.004_AHCI_02
- LAN Option ROM: 2.59
- Visual BIOS: 2.2.20

New Fixes/Features:

- Security enhancements.
- Fixed an issue where a BIOS hotkey would still work during boot, after enabling "Fast Boot".
- Fixed issue where USB keyboard or mouse can't wake up system from S5.

BIOS Version 0058 - TYBYT10H.86A.0058.2017.0329.2016

About This Release:

- Date: March 29, 2017
- ME Firmware: 1.0.2.1067
- Memory Reference Code: Based on 1.5.0
- Integrated Graphics
  - Option ROM: 36.2.5 Build 3757
  - UEFI Driver: 7.2.1008
- AHCI Code: Based on 5.004_AHCI_02
- LAN Option ROM: 2.59
- Visual BIOS: 2.2.20

New Fixes/Features:

- Added warning message if flashing the incorrect BIOS string.
- Security enhancements.

BIOS Version 0054 - TYBYT10H.86A.0054.2016.0929.1501

About This Release:

- Date: September 29, 2016
- TXE Firmware: 1.0.2.1067
- Framework BIOS Reference Code: Based on 1.5.0
- Integrated Graphics
  - Option ROM: 36.2.5 Build 3757
  - GOP Driver: 7.2.1008
- LAN
  - UEFI Driver: 2.0.26
- Visual BIOS: 2.2.20
- UEFI Revision: 2.3.1

New Fixes/Features:

- Security enhancements.

BIOS Version 0052 - TYBYT10H.86A.0052.2016.0822.1911

About This Release:

- Date: August 22, 2016
- TXE Firmware: 1.0.2.1067
- Framework BIOS Reference Code: Based on 1.5.0
- Integrated Graphics
  - Option ROM: 36.2.5 Build 3757

GOP Driver: 7.2.1008

- LAN
  UEFI Driver: 2.0.26
- Visual BIOS: 2.2.20
- UEFI Revision: 2.3.1

New Fixes/Features:

- Added auto recovery function by USB key feature.
- Added security enhancements.
- Fixed an issue where executing a reboot or shutdown - r command in Linux, the system would hang.
- Fixed the issue that when the user entered their password, and the "User Access Level = limited" the following restricted Setup options were still accessible:
  2.1 Minimum/Maximum Duty Cycle (%)
  2.2 2.2 Primary/secondary Temperature Sensor
  2.3 Pin 11/12/13/14/15/16
- Rolled back the TXE firmware from 1.0.5.1120 to 1.0.2.1067.
- Added G3 Power button recovery feature.
- Improved BIOS update function to disable keyboard and power button during flash/recovery process.
- Added Windows firmware update function.

Update Visual BIOS to 2.2.20 from 2.2.19.

- Hotfix to remove download driver and automatic BIOS update feature.
- Network capabilities will only work over LAN at this time.
- Opening a dropdown and changing screens can sometimes causes dropdown view to persist until an option is selected. This is a cosmetic error.

BIOS Version - TYBYT10H.86A.0049.2016.0413.1649

About This Release:

- Date: April 13, 2016
- TXE Firmware: 1.0.5.1120
- Framework BIOS Reference Code: Based on 1.5.0
- Integrated Graphics
  Option ROM: 36.2.5 Build 3757
  GOP Driver: 7.2.1008
- LAN
  UEFI Driver: 2.0.26
- Visual BIOS: 2.2.19
- UEFI Revision: 2.3.1

New Fixes/Features:

- Fixed the wrong OS selection option to follow spec.
- Fixed the issue where the OS selection can't be modified by ITK.
- Fixed the issue where VCUST would not work in DOS.
- Removed the "Pin function select for serial port header" section from the Legacy device configuration page.
- Fixed the issue where the computer that installs Wind River Linux can no longer use Putty to remote in to the Wind River system.

- Fixed the issue where the system can't resume from S3 in Windows 7 after updating the AmiModulePkg to 026 to support Secure Boot when PXE booting.
- Removed the mention of pin10 as GPIO, and the help string "Direct Application Launch feature".
- Removed the serial header from GPIO options.
- Updated Secure Boot to 014 so PXE boot can support Secure Boot
- Updated AmiModulePkg to 026 so PXE boot can support Secure Boot.

BIOS Version 0046 - TYBYT10H.86A.0046.2015.1014.1057

About This Release:

- Date: October 14, 2015
- TXE Firmware: 1.0.5.1120
- Framework BIOS Reference Code: Based on 1.5.0
- Integrated Graphics
  Option ROM: 36.2.5 Build 3757
  GOP Driver: 7.2.1008
- LAN
  UEFI Driver: 2.0.26
- Visual BIOS: 2.2.19
- UEFI Revision: 2.3.1

New Fixes/Features:

- Fixed poor performance issue that occurs after resuming from S3.
- Updated custom header solution setting.
- Fixed issue where monitor remains in sleep state after S3 wakeup from USB keyboard or mouse.
- Fixed issue where system does not wake from S3/S4 with RTV, when Wake from S5 is enabled.
- Fixed issue where a single CPU Thermal trip event is recorded twice in the event log.
- Changed the OS selection in BIOS from Windows 8.x to Windows 8.x/Windows10.
- Updated Intel Visual BIOS to version 2.2.19. Fixes include:
  - Hotfix to remove performance page accessibility from Atom-based NUC products.
  - Refactored graphics resolution algorithm to find closest supported resolution to 1024x768. This should correct scaling issues with 4K monitors.
  - Removed unused assets from Performance and Mainstream themes to reduce the overall size of Visual BIOS. Size savings should be around 300KB.
  - Fixed issue in Download Drivers feature where certain drivers were not visible if multiple attachments exist in the same record.
  - Fixed issue in Download Drivers feature where incorrect drivers would display if product was not found in database.
  - Fixed issue in Performance page that prevented additional workspaces from showing up (i.e. Memory Timings, etc.)
  - Fixed touch monitors not working correctly when display adapter supports greater than 1024x768 resolution.
  - Fixed AMT USB-R issue where absolute mouse position would not scale correctly in Visual BIOS.
- Fixed issue where USB ports fail in Linux* after upgrading to BIOS version 0040.

- Fixed issue where one of GPIO controllers is missing in Yocato* image.

TYBYT10H.86A.0044.2015.0701.1138 Production BIOS

About This Release:

- Date: July 01, 2015
- TXE Firmware: 1.0.5.1120
- Framework BIOS Reference Code: Based on 1.5.0
- Integrated Graphics
  Option ROM: 36.2.5 Build 3757
  GOP Driver: 7.2.1008
- LAN
  UEFI Driver: 2.0.26
- Visual BIOS: 2.2.13
- UEFI Revision: 2.3.1

New Fixes/Features:

1. Updated BIOS Reference Code to version 1.5.0
2. Implemented security enhancement solution.
3. Fixed issue with SDRAM/+5.0V Standby value detection.
4. Fixed issue with unattended BIOS configuration.

BIOS Version 0043 - TYBYT10H.86A.0043.2015.0323.1643

About This Release:

- Date: March 23, 2015
- TXE Firmware: 1.0.5.1120
- Framework BIOS Reference Code: Based on 1.3.8
- Integrated Graphics
  Option ROM: 36.2.5 Build 3757
  GOP Driver: 7.2.1008
- LAN
  UEFI Driver: 2.0.26
- Visual BIOS: 2.2.13
- UEFI Revision: 2.3.1

New Fixes/Features:

- Added BIOS security enhancements.
- Fixed issue where BIOS password prompts are not suppressed in Config Mode.
- Fixed issue with Power LED not blinking when the Thermal Trip warning is generated.
- Fixed issue where USB mouse doesn't work in DOS EDIT.
- Removed BIOS option to disable HDMI/DisplayPort Audio.
- Fixed Power Button Recovery issue under G3 mode.
- Fixed BIOSID issue under F7.
- Fixed issue where incorrect thermal event appears in the Event Log and shows a warning message during boot.
- Added "Suppress Alert Messages At Boot" item in Visual BIOS.

BIOS Version 0041 - TYBYT10H.86A.0041.2014.1224.1255

About This Release:

- Date: December 24, 2014

- TXE Firmware: 1.0.5.1120
- Framework BIOS Reference Code: Based on 1.3.8
- Integrated Graphics
  Option ROM: 36.2.5 Build 3757
  GOP Driver: 7.2.1008
- LAN
  UEFI Driver: 2.0.26
- Visual BIOS: 2.2.13
- UEFI Revision: 2.3.1

New Fixes/Features:

- Fixed issue with the Configure menu with the security jumper.

BIOS Version 0039 - TYBYT10H.86A.0039.2014.1211.1744

About This Release:

- Date: December 11, 2014
- TXE Firmware: 1.0.5.1120
- Framework BIOS Reference Code: Based on 1.3.8
- Integrated Graphics
  Option ROM: 36.2.5 Build 3757
  GOP Driver: 7.2.1008
- LAN
  UEFI Driver: 2.0.26
- Visual BIOS: 2.2.13
- UEFI Revision: 2.3.1

New Fixes/Features:

- Fixed USB communications failure with certain custom USB devices.

BIOS Version 0037 - TYBYT10H.86A.0037.2014.1120.1742

About This Release:

- Date: November 20, 2014
- TXE Firmware: 1.0.5.1120
- Framework BIOS Reference Code: Based on 1.3.8
- Integrated Graphics
  Option ROM: 36.2.5 Build 3757
  GOP Driver: 7.2.1008
- LAN
  UEFI Driver: 2.0.26
- Visual BIOS: 2.2.13
- UEFI Revision: 2.3.1

New Fixes/Features:

- Fixed reboot hang and spurious messages in Linux*.
- Updated TXE FW to version 1.0.5.1120.
- Updated Visual BIOS to version 2.2.13. Fixes include:
  - Fixed password input so that only A-Z, a-z, and 0-9 characters are accepted.
  - Fixed issue in screenshot function that caused final bitmap to be tinted blue.
  - Fixed issue in double-click boot feature that did not allow BIOS to boot to the correct device.
  - Fixed issue graphical error in dropdown box.

- Fixed hang on NUC Home Page 1 and Cooling Page when temp or voltage form contained no questions.
- Added variable check to determine whether or not to perform OS check before starting Visual Boot Manager.
- Fixed logic that caused beta opt-in request to keep popping up.
- Fixed various GUI issues.
- Fixed missing temperatures and voltages in cooling performance monitor.
- Fixed variable flags for OsIndications and BootNext to conform to strict UEFI 2.4 requirements.

BIOS Version 0036 - TYBYT10H.86A.0036.2014.1023.1022

About This Release:

- Date: October 23, 2014
- TXE Firmware: 1.0.2.1067
- Framework BIOS Reference Code: Based on 1.3.8
- Integrated Graphics
  Option ROM: 36.2.5 Build 3757
  GOP Driver: 7.2.1008
- LAN
  UEFI Driver: 2.0.26
- Visual BIOS: 2.2.8
- UEFI Revision: 2.3.1

New Fixes/Features:

- Fixed WHCK issues for Windows 7*.
- Added BIOS options:
  - S5 USB Power
  - Internal speaker
  - 4GB eMMC Built-in Storage
- Fixed issue with power button menu.
- Fixed issue where F10 boot menu shows incorrect information.
- Fixed issue where ACPI error appears in Event Log after installing the USB3.0 driver.
- Updated processor support.
- Updated GOP driver to version 7.2.1008.

BIOS Version 0034 - TYBYT10H.86A.0034.2014.0905.1747

About This Release:

- Date: September 5, 2014
- TXE Firmware: 1.0.2.1067
- Framework BIOS Reference Code: Based on 1.3.8
- Integrated Graphics
  Option ROM: 36.2.5 Build 3757
  GOP Driver: 7.2.1004
- LAN
  UEFI Driver: 2.0.26
- Visual BIOS: 2.2.8
- UEFI Revision: 2.3.1

New Fixes/Features:

- Fixed issue where performance is slow and sluggish.

BIOS Version 0032 - TYBYT10H.86A.0032.2014.0814.1913

About This Release:

- Date: August 14, 2014
- TXE Firmware: 1.0.2.1067
- Framework BIOS Reference Code: Based on 1.3.8
- Integrated Graphics
  Option ROM: 36.2.5 Build 3757
  GOP Driver: 7.2.1004
- LAN
  UEFI Driver: 2.0.26
- Visual BIOS: 2.2.8
- UEFI Revision: 2.3.1

New Fixes/Features:

- Speeded up BIOS update process – if Intel® ME version has not changed, that segment is skipped during update.
- Fixed issue where system does not boot or memory size is reported incorrectly with some SO-DIMM memory modules.
- Updated message when no bootable device is found.
- Add iSCSI feature.
- Updated Visual BIOS to version 2.2.8. Fixes include:
  - Fixed issue where Default BIOS Start Page would not show properly when selecting home pages.
  - Fixed hang when saving file using screenshot feature.
  - Fixed erroneous notification text when file save feature failed.
- Fixed issue where system gets stuck in reboot cycle after BIOS update.

BIOS Version 0030 - TYBYT10H.86A.0030.2014.0710.1012

About This Release:

- Date: July 10, 2014
- TXE Firmware: 1.0.2.1067
- Framework BIOS Reference Code: Based on 1.3.8
- Integrated Graphics
  Option ROM: 36.2.5 Build 3757
  GOP Driver: 7.2.1004
- LAN
  UEFI Driver: 2.0.26
- Visual BIOS: 2.2.7
- UEFI Revision: 2.3.1

New Fixes/Features:

- Updated AMI build tool (VEB) to the latest version for OA3 and ITK issues.
- Fixed HSUART device issue.
- Fixed issue where Windows Embedded Standard 7* fails in IDE mode.
- Fixed Windows 8 LPSS driver issues:
  - Set ACPI mode for Embedded Windows 8 in OS Selection
  - Remove the declaration of serial interface BT and GPS
- Updated VBIOS to version 36.2.5 Build 3757 and GOP to version 7.2.1004.
- Added Direct App Launch support.

- Updated Visual BIOS to version 2.2.7. Fixes include:
  - Fixed issue that caused startup hang when Default Start Page was set to Main Page.
  - Re-architected HTTP client in Visual BIOS to support network behind an HTTP proxy (i.e. corporate firewall) and handle network instability issues.
  - Updated performance pages to support simplified needs of NUC products going forward.
  - Fixed issue on settings page where NUC Atom theme was not an available option.
  - Fixed issue where default theme was not NUC theme if theme could not be determined.
  - Fixed issue where driver download feature could not be used after closing the modal and re-entering the modal.
- Fixed issue where Intel wireless adapters lose connectivity.
- Fixed issue where operating system installation fails with Intel 530 series SSD.

BIOS Version 0024 - TYBYT10H.86A.0024.2014.0523.1509

About This Release:

- Date: May 23, 2014
- TXE Firmware: 1.0.2.1067
- Framework BIOS Reference Code: Based on 1.3.6
- Integrated Graphics
  Option ROM: Build#3698
  GOP Driver: 7.1.1007
- LAN
  UEFI Driver: 2.0.26
- Visual BIOS: 2.2.5
- UEFI Revision: 2.3.1

New Fixes/Features:

- Fixed issue where system cannot enter S3 in Windows Embedded Standard 7*.
- Enhanced the protection of certain UEFI variables as described in Intel Security Advisory INTEL-SA-00038.
- Fixed Intel ME disable issue.
- Fixed issue where fan speed, temperature, and voltage are not reported in BIOS after modifying duty cycles.
- Fixed issue with BIOS password lengths.
- Updated 4GB eMMC built-in storage option.
- Fixed issue where the monitor will not display after S3 resume by USB keyboard/mouse or power button.
- Fixed issue where TXE test fails.
- Fixed issue where .BMP splash logo files do not display.
- Fixed issue where no error beeps or blinks occur when no memory modules are installed.
- Fixed issues with Wake on USB from S4/S5.
- Fixed issue where system will hang at POST code B2 when Startup Sound is enabled.
- Fixed issue where system hangs at POST code 71 after S3 resume.
- Modified default values associated with OS Selection options.
  - Windows 8.x - xHCI mode is enabled

    - Windows 7 - xHCI mode is set to "smart auto"; Legacy Boot is enabled and greyed out; Wake on USB from S4/S5 is disabled and greyed out
- Updated Visual BIOS to version 2.2.5. Fixes include:
    - Fixed issue where add-in config forms were unable to post changes to the setup browser.
    - Fixed issue with touch input that ignored the first touch state upon starting the application.
- Added Wake on USB from S4/S5 option.
- Fixed issue where system wakes up if USB hot-plugging in S5 state.
- Fixed issue where BIOS auto-update feature fails.
- Updated fan speed control.
- Added OS Selection option in Intel® Integrator Toolkit.
- Updated help text for OS Selection and USB Port.
- Added Serial Port option under Onboard Device tab.
- Fixed fan speed issue when resuming from S3.
- Fixed issue with disabling USB ports.
- Fixed issue where Wake on LAN from S4/S5 fails to Power on from PXE Boot.
- Fixed issue with On Board Devices Information related to auto-detection for WiFi
- Fixed issue with clearing TPM.

BIOS Version 0019 - TYBYT10H.86A.0019.2014.0327.1516

About This Release:

- Date: March 27, 2014
- TXE Firmware: 1.0.2.1067
- Framework BIOS Reference Code: Based on 1.3.4
- Integrated Graphics
  Option ROM: Build#3698
  GOP Driver: 7.1.1007
- LAN
  UEFI Driver: 2.0.26
- Visual BIOS: 2.2.4
- UEFI Revision: 2.3.1

New Fixes/Features:

- Initial production BIOS release

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