BIOS Update Release Notes

PRODUCTS: NUC10i7FN, NUC10i5FN, NUC10i3FN

BIOS Version 0063 – FNCML357.0063.2023.1024.1117

About This Release:

- Date: Oct 24, 2023
- ROM Image Checksum: 0xAB39EFE4
- EC Firmware: 03.12.00
- ME Firmware: 14.1.70.2228
- PMC Firmware: 140.1.1.1010
- i219 NVM: 0.8
- CRB Label: 1AWDV011
- Boot Guard ACM: V4532
- BIOS Guard: BiosGuard_009
- Silicon Initialization: 9.0.14.30
- Memory Reference Code: Based on 00.00.00.031
- Integrated Graphics:
  - Option ROM: 1021
  - UEFI Driver: 9.0.1107
- Intel RST Pre-OS:
  - UEFI Driver: 18.30.0.4502
- SATA RAID Option ROM: 17.8.0.4352
- AHCI Code: Based on AHCI_20
- LAN Option ROM: 0.0.24
- Visual BIOS: Intel AptioV

- Supported Flash Devices:

  Macronix MX25L25673GM2I-08G 32MB

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

  M80A0660_000000F8
  M94806EC_000000FA

Feature Changes/Updates/Fixes:

- Fixed issue where EDK2 PEI-Phase Denial of Service vulnerability.
- Fixed issue where Intel NUC TOCTOU vulnerability.
- Fixed issue where LogoFAIL vulnerability.
- Fixed issue where TOCTOU vulnerability in SmiFlash.
- Fixed issue where Intel NUC TOCTOU vulnerability-2.
- Updated Harden SMM Write Flash support.
- Fixed issue where Intel NUC information leak vulnerability.
- Updated OpenSSL Policy Constraints.
- Fixed issue where OOB RW vulnerability In select Intel NUC products.
- Updated CPU Microcode to M94806EC_000000FA.

Known Errata:

- Windows Bitlocker Recovery will occur after reloading of Secure Boot key in BIOS Setup since BIOS FN0062 includes an updated Secure Boot DBX.

BIOS Version 0062 - FNCML357.0062.2023.0719.2024

About This Release:

- Date: July 19, 2023
- ROM Image Checksum: 0xAAA0419D
- EC Firmware: 03.12.00
- ME Firmware: 14.1.70.2228
- PMC Firmware: 140.1.1.1010
- I219 NVM: 0.8
- CRB Label: 1AWDV011
- Boot Guard ACM: V4532
- BIOS Guard: BiosGuard_009
- Silicon Initialization: 9.0.14.30
- Memory Reference Code: Based on 00.00.00.031
- Integrated Graphics:
    - Option ROM: 1021
    - UEFI Driver: 9.0.1107
- Intel RST Pre-OS:
    - UEFI Driver: 18.30.0.4502
- SATA RAID Option ROM: 17.8.0.4352
- AHCI Code: Based on AHCI_20
- LAN Option ROM: 0.0.24
- Visual BIOS: Intel AptioV

- Supported Flash Devices:
  MACRONIX MX25L25673GM2I-08G 32MB

- Microcode Updates included in .BIN & .CAP Files:
  M80A0660_000000F8
  M94806EC_000000F8

Feature Changes/Updates/Fixes:

- Fixed issue where GRUB Bootloader vulnerability.
- Fixed issue where The stack buffer overflow vulnerability leads to arbitrary code execution in DXE driver on Intel platforms.
- Fixed issue where RSB Stuffing Mitigation for Speculative Execution vulnerability.
- Updated UEFI Boot Variables Access.
- Fixed issue where SDIO_DEV_CONFIGURATION SetVariable NVRAM Corruption.
- Fixed issue where UEFI Variable access vulnerability.
- Fixed issue where UEFI Variable access vulnerability in Intel NUC BIOS.
- Fixed issue where SmmEntryPoint Underflow vulnerability.
- Fixed issue where EDK2 vulnerabilities.
- Fixed issue where OpenSSL vulnerabilities.
- Fixed issue where Incorrect bound check vulnerability.

- Updated PlatformLang Timeout Variable Access.
- Updated SmiFlash related solution implementation.
- Updated SmiFlash related solutions including TOCTOU SmiFlash_v2.
- Updated OpenSSL Policy Constraints.
- Fixed issue where Heap Buffer Overflow in TCG2MeasurePeImage.
- Updated BlackLotus-SecureBoot DBX Update.
- Updated IPU 2023.1 Update.
- Updated IPU 2023.2 Update.
- Updated IPU 2023.3 Update.
- Fixed issue where iSetupCfg - WARNING: Duplicate questions.
- Updated BIOS Flash tool iFlashV 5.13.00.2106 (X64) / 5.13.00.2106 (Ia32).
- Updated ME FW to 14.1.70.2228.
- Updated CPU Microcodes to M94806EC_000000F8 and M80A0660_000000F8.

Known Errata:

- Windows Bitlocker Recovery will occur after reloading of Secure Boot key in BIOS Setup since BIOS FN0062 includes an updated Secure Boot DBX.

BIOS Version 0061 - FNCML357.0061.2023.0710.1812

About This Release:

- Date: July 14, 2023
- ROM Image Checksum: 0xAAC4A06B
- EC Firmware: 03.12.00
- ME Firmware: 14.1.67.2046
- PMC Firmware: 140.1.1.1010
- I219 NVM: 0.8
- CRB Label: 1AWDV011
- Boot Guard ACM: V4532
- BIOS Guard: BiosGuard_009
- Silicon Initialization: 9.0.14.30
- Memory Reference Code: Based on 00.00.00.031
- Integrated Graphics:
  - Option ROM: 1021
  - UEFI Driver: 9.0.1107
- Intel RST Pre-OS
  - UEFI Driver: 18.30.0.4502
- SATA RAID Option ROM: 17.8.0.4352
- AHCI Code: Based on AHCI_20
- LAN Option ROM: 0.0.24
- Visual BIOS: Intel AptioV

- Supported Flash Devices:

  MACRONIX MX25L25673GM2I-08G 32MB

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

  m80a0660_000000F0
  m94806ec_000000F4

Feature Changes/Updates/Fixes:

- Added Add new L10 SKU number in SMBIOS data area.

BIOS Version 0060 - FNCML357.0060.2023.0208.1148

About This Release:

- Date: Feb 08, 2023
- ROM Image Checksum: 0xAAD3DFCE
- EC Firmware: 03.12.00
- ME Firmware: 14.1.67.2046
- PMC Firmware: 140.1.1.1010
- I219 NVM: 0.8
- CRB Label: 1AWDV011
- Boot Guard ACM: V4532
- Bios Guard: BiosGuard_009
- Silicon Initialization: 9.0.14.30
- Memory Reference Code: Based on 00.00.00.031
- Integrated Graphics:
    - Option ROM: 1021
    - UEFI Driver: 9.0.1107
- Intel RST Pre-OS
    - UEFI Driver: 18.30.0.4502
- SATA RAID Option ROM: 17.8.0.4352
- AHCI Code: Based on AHCI_20
- LAN Option ROM: 0.0.24
- Visual BIOS: Intel AptioV

- Supported Flash Devices:

  MACRONIX MX25L25673GM2I-08G 32MB

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

  M80A0660_000000F0
  M94806EC_000000F0

Feature Changes/Updates/Fixes:

- Fixed issue where GRUB Bootloader Vulnerability.
- Updated 2022 IPU update: 2022.1/2022.3.
- Fixed issue where Intel NUC information disclosure vulnerability.
- Fixed issue OS Kernel-level malware may cause information disclosure vulnerability.
- Fixed issue where iSetupCfg tool was not able to change default value of PLx/Fan cuver parameters due to stdDefault override mechanism.
- Added Add StdDefaults into ProtectedNvVariableForRuntime ELink.
- Fixed issue where Building Process optimize_avoid UQI duplicated.

BIOS Version 0059 - FNCML357.0059.2022.1019.1055

About This Release:

- Date: Oct 21, 2022
- ROM Image Checksum: 80CF
- EC Firmware: 03.12.00
- ME Firmware: 14.1.67.2046
- PMC Firmware: 140.1.1.1010
- I219 NVM: 0.8
- CRB Label: 1AWDV011
- Boot Guard ACM: V4532
- Bios Guard: BiosGuard_009
- Silicon Initialization: 9.0.14.30
- Memory Reference Code: Based on 00.00.00.031
- Integrated Graphics:
    - Option ROM: 1021
    - UEFI Driver: 9.0.1107
- Intel RST Pre-OS:
    - UEFI Driver: 18.30.0.4502
- SATA RAID Option ROM: 17.8.0.4352
- AHCI Code: Based on AHCI_20
- LAN Option ROM: 0.0.24
- Visual BIOS: Intel AptioV

- Supported Flash Devices:
  MACRONIX MX25L25673GM2I-08G 32MB

- Microcode Updates included in .BIN & .CAP Files:
  M80A0660_000000F0
  M94806EC_000000F0

New Fixes/Features:

- Updated ME FW to 14.1.67.2046
- Fixed issue where Stack overflow vulnerability in SMI handler.
- Fixed issue where SMM memory corruption vulnerability in SMM driver on Intel platforms.
- Fixed issue where The arbitrary code execution in DXE driver.
- Fixed issue where Privilege escalation vulnerability from kernel to SMM in multiple devices.
- Fixed issue where TianoCore Security Issues.
- Fixed issue where Intel NUC 9 vulnerability.
- Fixed issue where SIO_DEV_STATUS_VAR_NAME Information Leakage.
- Fixed issue where Potential hack of EBU DLL.
- Fixed issue where Grub Bootloader Vulnerability.
- Fixed issue where vulnerability/info leak vulnerability.
- Updated CPU Microcode to M94806EC_000000F4 and M80A0660_000000F4.

BIOS Version 0058 - FNCML357.0058.2022.0720.1011

About This Release:

- Date: Jul 22, 2022
- ROM Image Checksum: DB2E
- ME Firmware: 14.1.65.1969

- EC Firmware: 03.12.00
- PMC Firmware: 140.1.01.1010
- Memory Reference Code: Based on RC9.0.14.30_011
- Integrated Graphics:
    - Option ROM: 1021
    - UEFI Driver: 9.0.1107
- SATA RAID Option ROM: 17.8.0.4352
- AHCI Code: Based on AHCI_20
- LAN Option ROM: 0.0.24
- Visual BIOS: Intel AptioV

- Supported Flash Devices:
  MACRONIX MX25L25673GM2I-08G 32MB

- Microcode Updates included in .BIN & .CAP Files:
  M80A0660_000000F0
  M94806EC_000000F0

New Fixes/Features:

- Updated "Press F6 to exist Manufacturing Mode" feature string update.
- Fixed issue where Buffer Overflow in UEFI Firmware BIOS core.
- Fixed issue where Information disclosure vulnerability.
- Fixed issue where System always reset loop after RTC power loss.
- Fixed issue where Arbitrary write vulnerability in PEI module leads to arbitrary code execution in PEI phase.
- Fixed issue where PEI memory corruption on server boards and on majority of NUCs.
- Added Patch for a message warning when a system upgrade means a downgrade is no possible.
- Added "BootPerformanceTable_pointer".
- Fixed issue where POST Hotkey message does not display with Secure Boot enabled.
- Updated EC FW to 03.12.00.
- Updated Unified "OemCommonLib.h" reference file.

BIOS Version 0057 - FNCML357.0057.2022.0520.1803

About This Release:

- Date: May 20, 2022
- ROM Image Checksum: 0774
- ME Firmware: 14.1.65.1969
- EC Firmware: 03.11.00
- PMC Firmware: 140.1.01.1010
- Memory Reference Code: Based on RC9.0.14.30_011
- Integrated Graphics:
    - Option ROM: 1021
    - UEFI Driver: 9.0.1107
- SATA RAID Option ROM: 17.8.0.4352
- AHCI Code: Based on AHCI_20
- LAN Option ROM: 0.0.24
- Visual BIOS: Intel AptioV

- Supported Flash Devices:
  MACRONIX MX25L25673GM2I-08G 32MB

- Microcode Updates included in .BIN & .CAP Files:
  M80A0660_000000F0
  M94806EC_000000F0

New Fixes/Features:

- Updated ME Firmware to 14.1.65.1969.

- Updated to CPU Microcode updated to M80A0660_000000F0 and M94806EC_000000F0
- Updated EC Firmware to 03.11.00
- Fixed issue where system can't boot up after changing settings.
- Fixed issue where Timer does not restart NUC under Ubuntu Linux 20.04 (LTS).
- Implemented Config Mode load safe settings.
- Added Event Log code check for feature "Press F6 from BIOS setup to exit MFG mode".
- Added OpenSSL version check if been updated to CryptoPkg_37.
- Fixed patch for BIOS Warning message during BIOS update from Windows Update (Follow Master RD3.10).

BIOS Version 0056 - FNCML357.0056.2022.0223.1614

About This Release:

- Date: Feb 23, 2022
- ROM Image Checksum: 4704
- ME Firmware: 14.0.47.1558
- EC Firmware: 03.09.00
- PMC Firmware: 140.1.01.1010
- Memory Reference Code: Based on RC9.0.14.30_011
- Integrated Graphics:
  - Option ROM: 1021
  - UEFI Driver: 9.0.1107
- SATA RAID Option ROM: 17.8.0.4352
- AHCI Code: Based on AHCI_20
- LAN Option ROM: 0.0.24
- Visual BIOS: Intel AptioV

- Supported Flash Devices:
  MACRONIX MX25L25673GM2I-08G 32MB

- Microcode Updates included in .BIN & .CAP Files:
  m80a0660_000000ea
  m94806ec_000000ec

New Fixes/Features:

- Fixed issue where NUC failed (no boot) after several reboot attempts.
- Added functionality when pressing “F6” from BIOS Setup will exit MFG mode.
- Updated CPU Microcode (0xEC/0xEA) for IPU 2021.2
- Updated 2021.2 IPU BIOS change.
- Updated Self-Help feature.

BIOS Version 0055 - FNCML357.0055.2021.1202.1748

About This Release:

- Date: Dec 02, 2021
- ROM Image Checksum: AA86370E
- ME Firmware: 14.0.47.1558
- EC Firmware: 03.09.00
- PMC Firmware: 140.1.01.1010
- Memory Reference Code: Based on RC9.0.14.30_011
- Integrated Graphics:
  - Option ROM: 1021
  - UEFI Driver: 9.0.1107
- SATA RAID Option ROM: 17.8.0.4352
- AHCI Code: Based on AHCI_20
- LAN Option ROM: 0.0.24

- Visual BIOS: Intel AptioV

- Supported Flash Devices:
  MACRONIX MX25L25673GM2I-08G 32MB

- Microcode Updates included in .BIN & .CAP Files:
  m80a0660_000000e8
  m94806ec_000000ea

New Fixes/Features:

- Added Pop-Up warning message to User when transition BIOS is necessary.
- Fixed issue with FX System Verification Test.
- Fixed issue where system wakes on USB even with wake on USB S5 disabled.
- Fixed issued where unauthorized modification of UEFI variables could disable the protect mechanism of SMM.
- Fixed issue where BIOS could not update version FN0052 to FN0053 in headless mode.

BIOS Version 0053 - FNCML357.0053.2021.0707.1420

About This Release:

- Date: Jul 7, 2021
- ROM Image Checksum: dd32d385
- ME Firmware: 14.0.47.1558
- EC Firmware: 03.09.00
- PMC Firmware: 140.1.01.1010
- Memory Reference Code: Based on RC9.0.14.30_011
- Integrated Graphics:
  - Option ROM: 1021
  - UEFI Driver: 9.0.1093
- SATA RAID Option ROM: 17.8.0.4352
- AHCI Code: Based on AHCI_20
- LAN Option ROM: 0.0.24
- Visual BIOS: Intel AptioV

- Supported Flash Devices:
  - MACRONIX MX25L25673GM2I-08G 32MB

- Microcode Updates included in .BIN & CAP Files:
  - m80a0660_000000e8
  - m94806ec_000000ea

New Fixes/Features:

- **Fixed**: Cannot enable/disable "Fast Boot".
- **Fixed**: Issue where the Intel NUC won't boot if you set IGD Aperture size to 2048 and disable UEFI boot.
- **Updated**: Updated CPU Microcode to m80a0660_000000e8 and m94806ec_000000ea.
- **Updated**: BNIOS security.

BIOS Version 0052 - FNCML357.0052.2021.0409.1144

About This Release:

- Date: April 09, 2021
- ROM Image Checksum: 0xB99D
- ME Firmware: 14.0.47.1558
- EC Firmware: 03.09.00
- PMC Firmware: 140.1.01.1010

- Memory Reference Code: Based on RC9.0.14.30_011
- Integrated Graphics:
    - Option ROM: 1021
    - UEFI Driver: 9.0.1093
- SATA RAID Option ROM: 17.8.0.4352
- AHCI Code: Based on AHCI_20
- LAN Option ROM: 0.0.24
- Visual BIOS: Intel AptioV

- Supported Flash Devices:
  MACRONIX MX25L25673GM2I-08G 32MB

- Microcode Updates included in .BIN & .CAP Files:
  M94806EC_000000DE.pdb
  M80A0660_000000E0.pdb

New Fixes/Features:

- Enabled Thunderbolt boot support after a "F7" BIOS update.
- Fixed issue regarding no display during POST when only using a Thunderbolt / Type-C to HDMI adapter.

BIOS Version 0051 - FNCML357.0051.2021.0324.1859

About This Release:

- Date: Mar 24, 2021
- ROM Image Checksum: 0x05BF
- ME Firmware: 14.0.47.1558
- EC Firmware: 03.09.00
- PMC Firmware: 140.1.01.1010
- Memory Reference Code: Based on RC9.0.14.30_011
- Integrated Graphics:
    - Option ROM: 1021
    - UEFI Driver: 9.0.1093
- SATA RAID Option ROM: 17.8.0.4352
- AHCI Code: Based on AHCI_20
- LAN Option ROM: 0.0.24
- Visual BIOS: Intel AptioV

- Supported Flash Devices:
  MACRONIX MX25L25673GM2I-08G 32MB

- Microcode Updates included in .BIN & .CAP Files:
  M94806EC_000000DE.pdb
  M80A0660_000000E0.pdb

New Fixes/Features:

- Fixed issue recognizing a USB device on a Thunderbolt dock after rebooting.
- Fixed issue with audio codec default setup.
- Updated NTFS DXE driver when parsing NTFS file system partition.

BIOS Version 0050 - FNCML357.0050.2021.0303.2146

About This Release:

- Date: Mar 03, 2021
- ROM Image Checksum: 0x2E14
- ME Firmware: 14.0.47.1558
- EC Firmware: 03.09.00
- PMC Firmware: 140.1.01.1010
- Memory Reference Code: Based on RC9.0.14.30_011
- Integrated Graphics:
    - Option ROM: 1021
    - UEFI Driver: 9.0.1093
- SATA RAID Option ROM: 17.8.0.4352
- AHCI Code: Based on AHCI_20
- LAN Option ROM: 0.0.24
- Visual BIOS: Intel AptioV

- Supported Flash Devices:
  MACRONIX MX25L25673GM2I-08G 32MB

- Microcode Updates included in .BIN & .CAP Files:
  M94806EC_000000DE.pdb
  M80A0660_000000E0.pdb

New Fixes/Features:

- Updated Audio Codec software.
- Updated GBE (Gigabit Ethernet) to 0.8 and fixed incorrect SSID issue.
- Updated ME firmware to 14.0.47.1558

Known Errata:

- Due to the Intel® ME firmware update in BIOS version 0050, you can’t downgrade to version 0047 or earlier.

BIOS Version 0047 - FNCML357.0047.2020.1118.1629

About This Release:

- Date: Nov 18, 2020
- ROM Image Checksum: 0xC7CC
- ME Firmware: 14.0.45.1389
- EC Firmware: 03.09.00
- PMC Firmware: 140.1.01.1010
- Memory Reference Code: Based on RC9.0.14.30_011
- Integrated Graphics:
    - Option ROM: 1021
    - UEFI Driver: 9.0.1093
- SATA RAID Option ROM: 17.8.0.4352
- AHCI Code: Based on AHCI_20
- LAN Option ROM: 0.0.24
- Visual BIOS: Intel AptioV

- Supported Flash Devices:
  MACRONIX MX25L25673GM2I-08G 32MB

- Microcode Updates included in .BIN & .CAP Files:
  M94806EC_000000DE.pdb
  M80A0660_000000E0.pdb

New Fixes/Features:

- Updated the ME firmware to 14.0.45.1389
- Updated the EC firmware to 03.09.00
- Added Self-healing BIOS code.
- Fixed the issue where "New SOC I5 load line Fail".
- Fixed issue to control "RING LED" and "HDD LED" via WMI method.
- Updated BIOS code for security fixes.

BIOS Version 0046 - FNCML357.0046.2020.0928.1457

About This Release:

- Date: Sept 28, 2020
- ROM Image Checksum: 0xF2F8
- ME Firmware: 14.0.39.1339
- EC Firmware: 03.07.00
- PMC Firmware: 140.1.01.1010
- Memory Reference Code: Based on RC9.0.14.30_011
- Integrated Graphics:
    - Option ROM: 1021
    - UEFI Driver: 9.0.1093
- SATA RAID Option ROM: 17.8.0.4352
- AHCI Code: Based on AHCI_20
- LAN Option ROM: 0.0.24
- Visual BIOS: Intel AptioV

- Supported Flash Devices:
  MACRONIX MX25L25673GM2I-08G 32MB

- Microcode Updates included in .BIN & .CAP Files:
  M94806EC_000000D6.pdb
  M80A0660_000000CA.pdb

New Fixes/Features:

- Fixed issue updating BIOS using "F7" update method.

BIOS Version 0045 - FNCML357.0045.2020.0817.1709

About This Release:

- Date: Aug 17, 2020
- ROM Image Checksum: 0x2F4D
- ME Firmware: 14.0.39.1339
- EC Firmware: 03.07.00
- PMC Firmware: 140.1.01.1010
- Memory Reference Code: Based on RC9.0.14.30_011
- Integrated Graphics:
    - Option ROM: 1021
    - UEFI Driver: 9.0.1093
- SATA RAID Option ROM: 17.8.0.4352
- AHCI Code: Based on AHCI_20
- LAN Option ROM: 0.0.24
- Visual BIOS: Intel AptioV

- Supported Flash Devices:
  MACRONIX MX25L25673GM2I-08G 32MB

- Microcode Updates included in .BIN & .CAP Files:
  M94806EC_000000D6.pdb
  M80A0660_000000CA.pdb

New Fixes/Features:

- Updated ME Firmware to 14.0.39.1339
- Fixed issue with "iSetupCfg" log file.
- Fixed issue where failure to image by SCCM.
- Fixed issue with watchdog not clearing counter.
- Fixed issue where BIOS Self Recovery must be disabled if Failsafe Watchdog is disabled.

Known Errata:

- Due to the Intel® ME firmware update in BIOS version 0045, you can't downgrade to version 0044 or earlier.

BIOS Version 0044 - FNCML357.0044.2020.0715.1813

About This Release:

- Date: July 15, 2020
- ROM Image Checksum: 0x704E
- ME Firmware: 14.0.34.1139
- EC Firmware: 03.07.00
- PMC Firmware: 140.1.01.1010
- Memory Reference Code: Based on RC9.0.14.30_011
- Integrated Graphics:
  - Option ROM: 1021
  - UEFI Driver: 9.0.1093
- SATA RAID Option ROM: 17.8.0.4352
- AHCI Code: Based on AHCI_20
- LAN Option ROM: 0.0.24
- Visual BIOS: Intel AptioV

- Supported Flash Devices:
  MACRONIX MX25L25673GM2I-08G 32MB

- Microcode Updates included in .BIN & .CAP Files:
  M94806EC_000000CA.pdb
  M80A0660_000000CA.pdb

New Fixes/Features:

- Fixed issue with Thunderbolt boot default need to change from Enable to Disable to speed up BIOS POST time.
- Fixed issue with incorrect BIOS Setup Temperature display.
- Fixed issue affecting BIOS Optane settings not allowing for OS boot.
- Updated BIOS code for security fixes and improvements.
- Fixed issue PXE boot error display message.
- Fixed issue to disable TPM/PTT at BIOS level.
- Fixed issue to install Windows 10 SCCM.
- Updated ME Firmware version to 14.0.34.1139
- Updated TBT boot default from enable to disable.
- Fixed "iSetupCfg" map string error.
- Updated BIOS and EC Firmware to improve RTC_Reset functionality.

- Fixed "iSetupcfg" token dump issue, setup items and password check item issue.
- Fixed issue when BIOS detected no memory and prompt a warning message, BIOS will disable WDT to prevent from reset.
- Fixed Energy Star Logo issue for "BXNUC10i5FNHCA" SKU.
- Removed RAM Disk from BIOS setup.
- Fixed "Strings of Tau" value to meet SPEC requirement.
- Fixed CMOS Time overflow issue when switching SSD between different systems.
- Updated BIOS setup to provide URL address and QR code availability leading to NUC support webpage.
- Updated BIOS Screen and Power Button Menu.

Known Errata:

- Due to the Intel® ME firmware update in BIOS version 0044, you can't downgrade to version 0039 or earlier.

BIOS Version 0039 - FNCML357.0039.2020.0312.1734

About This Release:

- Date: March 12, 2020
- ROM Image Checksum: 0xB98F
- ME Firmware: 14.0.31.1120
- EC Firmware: 03.04.00
- PMC Firmware: 140.1.01.1008
- Memory Reference Code: Based on RC9.0.14.30_011
- Integrated Graphics:
  - Option ROM: 1021
  - UEFI Driver: 9.0.1093
- SATA RAID Option ROM: 17.8.0.4352
- AHCI Code: Based on AHCI_20
- LAN Option ROM: 0.0.24
- Visual BIOS: Intel AptioV

- Supported Flash Devices:

  MACRONIX MX25L25673GM2I-08G 32MB

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

  M94806EC_000000C6.mcb
  M80A0660_000000C6.mcb

New Fixes/Features:

- ME Firmware updated to 14.0.31.1120.
- Fixed issue regarding SCE tool setup.

BIOS Version 0038 - FNCML357.0038.2020.0131.1422

About This Release:

- Date: January 31, 2020
- ROM Image Checksum: 0x43D7
- ME Firmware: 14.0.0.1061
- EC Firmware: 03.04.00
- PMC Firmware: 140.1.01.1004

- Memory Reference Code: Based on RC9.0.14.30_011
- Integrated Graphics:
    - Option ROM: 1021
    - UEFI Driver: 9.0.1093
- SATA RAID Option ROM: 17.8.0.4352
- AHCI Code: Based on AHCI_20
- LAN Option ROM: 0.0.24
- Visual BIOS: Intel AptioV

- Supported Flash Devices:
  MACRONIX MX25L25673GM2I-08G 32MB

- Microcode Updates included in .BIN & .CAP Files:
  M94806EC_000000C6.mcb
  M80A0660_000000C6.mcb

New Fixes/Features:

- Fixed issue with BIOS fault tolerance failing after BIOS is re-signed.

BIOS Version 0037 - FNCML357.0037.2019.1226.1738

About This Release:

- Date: December 26, 2019
- ROM Image Checksum: 0x7035
- ME Firmware: 14.0.0.1061
- EC Firmware: 03.04.00
- PMC Firmware: 140.1.01.1004
- Memory Reference Code: Based on RC9.0.14.30_011
- Integrated Graphics:
    - Option ROM: 1021
    - UEFI Driver: 9.0.1093
- SATA RAID Option ROM: 17.8.0.4352
- AHCI Code: Based on AHCI_20
- LAN Option ROM: 0.0.24
- Visual BIOS: Intel AptioV

- Supported Flash Devices:
  MACRONIX MX25L25673GM2I-08G 32MB

- Microcode Updates included in .BIN & .CAP Files:
  M94806EC_000000C6.mcb
  M80A0660_000000C6.mcb

New Fixes/Features:

- Updated BIOS code for security fixes.
- Fixed HDD LED functionality issue.

BIOS Version 0036 - FNCML357.0036.2019.1207.1504

About This Release:

- Date: December 07, 2019
- ROM Image Checksum: 0x27C0

- ME Firmware: 14.0.0.1061
- EC Firmware: 03.04.00
- PMC Firmware: 140.1.01.1004
- Memory Reference Code: Based on RC9.0.14.30_011
- Integrated Graphics:
    - Option ROM: 1021
    - UEFI Driver: 9.0.1093
- SATA RAID Option ROM: 17.8.0.4352
- AHCI Code: Based on AHCI_20
- LAN Option ROM: 0.0.24
- Visual BIOS: Intel AptioV

- Supported Flash Devices:
  MACRONIX MX25L25673GM2I-08G 32MB

- Microcode Updates included in .BIN & .CAP Files:
  M94806EC_000000C6.mcb
  M80A0660_000000C6.mcb

New Fixes/Features:

- Fixed issue with setup of SATA M.2 device.
- Updated BIOS code for security fixes.
- Added "2.7 Notification of LED App".
- Added multiple features to enhance LED capabilities.
- Added "SetupNvLock" for Frost Canyon.
- Fixed issue with ESA/F7.
- Fixed issue with PXE.
- Fixed NVMe recovery issue if TBT enabled.
- Fixed BIOS recovery issue.
- Updated BIOS code for SGX function.
- Fixed Cortana can't wake from Modern Standby issue.

BIOS Version 0032 - FNCML357.0032.2019.1021.1624

About This Release:

- Date: October 21, 2019
- ROM Image Checksum: 0x1DE9
- ME Firmware: 14.0.0.1061
- EC Firmware: 03.04.00
- PMC Firmware: 140.1.01.1004
- Memory Reference Code: Based on RC9.0.14.30_011
- Integrated Graphics:
    - Option ROM: 1021
    - UEFI Driver: 9.0.1093
- SATA RAID Option ROM: 17.8.0.4352
- AHCI Code: Based on AHCI_20
- LAN Option ROM: 0.0.24
- Visual BIOS: Intel AptioV

- Supported Flash Devices:
  MACRONIX MX25L25673GM2I-08G 32MB

- Microcode Updates included in .BIN & .CAP Files:
  M94806EC_000000C6.mcb

M80A0660_000000C6.mcb

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.

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