BIOS Update Release Notes

PRODUCTS: NUC8CCHKR, NUC8CCHB

BIOS Version 0054 - CHAPLCEL.0054.2021.0512.1532

About This Release:

- Date: May 12, 2021
- ROM Image Checksum: 0x76BB
- TXE Firmware: 3.1.80.2400
- PMC Firmware: 03.1F
- EC1 Firmware: 0D.22.00
- EC2 Firmware: 0D.21.00
- Framework Reference Code: Based on 1.4.6
- Integrated Graphics:
    - Option ROM: Build 10.0.1016
    - UEFI Driver: 10.0.1037
- LAN Option ROM: i211 GbE
- Visual BIOS: Intel AptioV

- Supported Flash Devices:

Win Bond	W25Q128FWSIQ	16 MB (1.8V)
GD	GD25LB128DSIGR	16 MB (1.8V)
MACRONIX	MX25U12873FM2I-10G	16 MB (1.8V)

- Microcode Updates included in .BIN & .CAP Files:
  M03506C9_00000044.PDB
  M03506CA_00000020.PDB

New Fixes/Features:

- Added protection code for unauthorized write at controllable address in SMRAM.
- Fixed issue to achieve arbitrary write in SMRAM save state region.
- Updated CPU Microcode to M03506C9_00000044.PDB and M03506CA_00000020.PDB

BIOS Version 0053 - CHAPLCEL.0053.2021.0318.1408

About This Release:

- Date: Mar 18, 2021
- ROM Image Checksum: 0xE436
- TXE Firmware: 3.1.80.2400
- PMC Firmware: 03.1F
- EC1 Firmware: 0D.22.00
- EC2 Firmware: 0D.21.00
- Framework Reference Code: Based on 1.4.6
- Integrated Graphics:
    - Option ROM: Build 10.0.1016
    - UEFI Driver: 10.0.1037
- LAN Option ROM: i211 GbE

- Visual BIOS: Intel AptioV

- Supported Flash Devices:

Win Bond	W25Q128FWSIQ	16 MB (1.8V)
GD	GD25LB128DSIGR	16 MB (1.8V)
MACRONIX	MX25U12873FM2I-10G	16 MB (1.8V)

- Microcode Updates included in .BIN & .CAP Files:
  M03506C9_00000040.PDB
  M03506CA_0000001E.PDB

New Fixes/Features:

- Fixed issue to notify the EC to stop EC watchdog timer counter
- Updated ME Firmware to 3.1.80.2400
- Fixed issue with NTFS DXE driver when parsing NTFS file system partition.
- Fixed issue with Timeout Variable implementation.
- Fixed duplication issue with iSetupCfg.

Known Errata:

- Due to the Intel® ME firmware update in BIOS version 0053, you can't downgrade to version 0051 or earlier.

BIOS Version 0051 - CHAPLCEL.0051.2020.1022.1522

About This Release:

- Date: Oct 21, 2020
- ROM Image Checksum: 0x65CB
- TXE Firmware: 3.1.76.2356
- PMC Firmware: 03.1F
- EC1 Firmware: 0D.22.00
- EC2 Firmware: 0D.21.00
- Framework Reference Code: Based on 1.4.6
- Integrated Graphics:
  - Option ROM: Build 10.0.1016
  - UEFI Driver: 10.0.1037
- LAN Option ROM: i211 GbE
- Visual BIOS: Intel AptioV

- Supported Flash Devices:

Win Bond	W25Q128FWSIQ	16 MB (1.8V)
GD	GD25LB128DSIGR	16 MB (1.8V)
MACRONIX	MX25U12873FM2I-10G	16 MB (1.8V)

- Microcode Updates included in .BIN & .CAP Files:
  M03506C9_00000040.PDB
  M03506CA_0000001E.PDB

New Fixes/Features:

- Fixed issue with arbitrary code execution during PEI phase (WakeUpType).
- Fixed issue in "iSetupCfg" where duplicate "Map String" in BIOS prevented BIOS customization.

BIOS Version 0050 - CHAPLCEL.0050.2020.0812.1024

About This Release:

- Date: Aug 13, 2020
- ROM Image Checksum: 0xDB40
- TXE Firmware: 3.1.76.2356
- PMC Firmware: 03.1F
- EC1 Firmware: 0D.22.00
- EC2 Firmware: 0D.21.00
- Framework Reference Code: Based on 1.4.6
- Integrated Graphics:
    - Option ROM: Build 10.0.1016
    - UEFI Driver: 10.0.1037
- LAN Option ROM: i211 GbE
- Visual BIOS: Intel AptioV

- Supported Flash Devices:

Win Bond	W25Q128FWSIQ	16 MB (1.8V)
GD	GD25LB128DSIGR	16 MB (1.8V)
MACRONIX	MX25U12873FM2I-10G	16 MB (1.8V)

- Microcode Updates included in .BIN & .CAP Files:
  M03506C9_0000003C.PDB
  M03506CA_0000001C.PDB

New Fixes/Features:

- Fixed issue with "iSetupCfg" dump file.
- Fixed issue with functionality of "CH BIOS Power button control".
- Updated BIOS code for security fixes.
- Fixed issue where BIOS watchdog counter was not clearing.
- Fixed issue where BIOS Self Recovery must be disabled if Failsafe Watchdog is disabled.
- Updated ME/TXE firmware to 3.1.76.2356

BIOS Version 0049 - CHAPLCEL.0049.2020.0527.1654

About This Release:

- Date: May 27, 2020
- ROM Image Checksum: 0x5A7C
- TXE Firmware: 3.1.70.2334
- PMC Firmware: 03.1F
- EC1 Firmware: 0D.22.00
- EC2 Firmware: 0D.21.00
- Framework Reference Code: Based on 1.4.6
- Integrated Graphics:
    - Option ROM: Build 10.0.1016
    - UEFI Driver: 10.0.1037
- LAN Option ROM: i211 GbE
- Visual BIOS: Intel AptioV

- Supported Flash Devices:

Win Bond	W25Q128FWSIQ	16 MB (1.8V)
GD	GD25LB128DSIGR	16 MB (1.8V)
MACRONIX	MX25U12873FM2I-10G	16 MB (1.8V)

- Microcode Updates included in .BIN & .CAP Files:
  M03506C9_0000003C.PDB
  M03506CA_0000001C.PDB

New Fixes/Features:

- Fixed issue where "iSetupCfg" did not generate full list of UQI values.
- Fixed issue where "BIOS Allow UEFI 3rd party driver loaded description different with Spec".
- Fixed issue in "iSetup" regarding BIOS SCE spec.
- Fixed issue where "iSetupCfg" records fails on internal shell.
- Fixed issue where while disabling Front Panel USB3 port still can detect USB 3 device in OS.
- Fixed issue where AC 8265 Adapter disappears in windows after soft reboot.

BIOS Version 0048 - CHAPLCEL.0048.2020.0225.1640

About This Release:

- Date: Feb 26, 2020
- ROM Image Checksum: 0xA48A
- TXE Firmware: 3.1.70.2334
- PMC Firmware: 03.1F
- EC1 Firmware: 0D.22.00
- EC2 Firmware: 0D.21.00
- Framework Reference Code: Based on 1.4.6
- Integrated Graphics:
  - Option ROM: Build 10.0.1016
  - UEFI Driver: 10.0.1037
- LAN Option ROM: i211 GbE
- Visual BIOS: Intel AptioV

- Supported Flash Devices:

Win Bond	W25Q128FWSIQ	16 MB (1.8V)
GD	GD25LB128DSIGR	16 MB (1.8V)
MACRONIX	MX25U12873FM2I-10G	16 MB (1.8V)

- Microcode Updates included in .BIN & .CAP Files:
  M03506C9_0000003C.PDB
  M03506CA_0000001C.PDB

New Fixes/Features:

- Fixed issue where "Recovery DrawLogo arithmetic overflow/underflow."
- Fixed issue where "When S0 Indicator Brightness not set at default, after boot it will stay at 100% LED on."
- Fixed issue where "Power LED will turn off when used in a particular way to release power button."
- Implement EC1 firmware 2200.
- Updated TXE to 3.1.70.2334.

BIOS Version 0047 - CHAPLCEL.0047.2019.1230.2149

About This Release:

- Date: Dec 24, 2019
- ROM Image Checksum: 0x8A23
- TXE Firmware: 3.1.70.2331
- PMC Firmware: 03.1F
- EC1 Firmware: 0D.21.00
- EC2 Firmware: 0D.21.00
- Framework Reference Code: Based on 1.4.6
- Integrated Graphics:
    - Option ROM: Build 10.0.1016
    - UEFI Driver: 10.0.1037
- LAN Option ROM: i211 GbE
- Visual BIOS: Intel AptioV

- Supported Flash Devices:

Win Bond	W25Q128FWSIQ	16 MB (1.8V)
GD	GD25LB128DSIGR	16 MB (1.8V)
MACRONIX	MX25U12873FM2I-10G	16 MB (1.8V)

- Microcode Updates included in .BIN & .CAP Files:
  M03506C9_0000003C.PDB
  M03506CA_0000001C.PDB

New Fixes/Features:

- EC Firmware Update.
- Updated BIOS code for security fixes.
- Added "S4/S5 deep" option in BIOS and set default to enable.
- Added MCU version display "0" in setup menu.

BIOS Version 0046 - CHAPLCEL.0046.2019.1209.0929

About This Release:

- Date: Dec 09, 2019
- ROM Image Checksum: 0x6F6A
- TXE Firmware: 3.1.70.2331
- PMC Firmware: 03.1F
- EC1 Firmware: 0D.20.00
- EC2 Firmware: 0D.19.00
- Integrated Graphics:
    - Option ROM: Build 10.0.1016
    - UEFI Driver: 10.0.1037
- Framework Reference Code: Based on 1.4.6
- LAN Option ROM: i211 GbE
- Visual BIOS: Intel AptioV

- Supported Flash Devices:

Win Bond	W25Q128FWSIQ	16 MB (1.8V)
GD	GD25LB128DSIGR	16 MB (1.8V)
MACRONIX	MX25U12873FM2I-10G	16 MB (1.8V)

- Microcode Updates included in .BIN & .CAP Files:
  M03506C9_0000003C.PDB

New Fixes/Features:

- Implemented eMMC and NVME erase protocol.
- Implemented new BWG RC code change for USB part.
- Added "EnDebugMode" token and USE_PRIVATE_KEY = 1 for the resign.
- Fixed issue with NVME module.

BIOS Version 0044 - CHAPLCEL.0044.2019.1118.1625

About This Release:

- Date: Nov 18, 2019
- ROM Image Checksum: 0x2DC4
- TXE Firmware: 3.1.70.2331
- PMC Firmware: 03.1F
- EC1 Firmware: 0D.20.00
- EC2 Firmware: 0D.19.00
- Integrated Graphics:
    - Option ROM: Build 10.0.1016
    - UEFI Driver: 10.0.1037
- Framework Reference Code: Based on 1.4.6
- LAN Option ROM: i211 GbE
- Visual BIOS: Intel AptioV

- Supported Flash Devices:

WinBond	W25Q128FWSIQ	16 MB (1.8V)
GD	GD25LB128DSIGR	16 MB (1.8V)
MACRONIX	MX25U12873FM2I-10G	16 MB (1.8V)

- Microcode Updates included in .BIN & .CAP Files:
  M03506C9_0000003C.PDB

New Fixes/Features:

- Removed the NVME erase protocol.
- Rollback TPM (Trusted Platform Module) solution.
- Fixed issue after SMBIOS reboot.
- Fixed buffer overflow in Intel NUC UEFI modules “AcpiPlatform”.
- Changed the LED policy per product spec definition.
- If the board hardware supports the single-color power LED, the LED will be on for the first 3 seconds. After 3 seconds, the LED pattern follows the pattern: 25 seconds off, .25 seconds on, .25 seconds off, .25 seconds on to signal the user to release the power button.
- Changed the EC register 0x4FA from 0x64 to 0x5A and 0x4FB from 0x05 to 0x01.
- Set the BIT0 of general PM configuration 1 when the AFU tool send MU or ML command.
- Adjusted wake on LAN after G3.
- Adjusted power button menu LED policy to align Master RD spec.
- Implemented Block Erase support in NVMe driver.
- Implemented EFI_ERASE_BLOCK_PROTOCOL support in AHCI driver.
- Set command port to 0x07 for access memory and I/O space

BIOS Version 0038 - CHAPLCEL.0038.2019.0923.1810

About This Release:

- Date: Sep 23, 2019

- ROM Image Checksum: 0x7FB1
- TXE Firmware: 3.1.70.2331
- PMC Firmware: 03.1F
- EC1 Firmware: 0D.20.00
- EC2 Firmware: 0D.19.00
- Integrated Graphics:
    - Option ROM: Build 10.0.1016
    - UEFI Driver: 10.0.1037
- Framework Reference Code: Based on 1.4.6
- LAN Option ROM: i211 GbE
- Visual BIOS: Intel AptioV

- Supported Flash Devices:

WinBond	W25Q128FWSIQ	16 MB (1.8V)
GD	GD25LB128DSIGR	16 MB (1.8V)
MACRONIX	MX25U12873FM2I-10G	16 MB (1.8V)

- Microcode Updates included in .BIN & .CAP Files:
  M03506C9_0000003C.PDB

New Fixes/Features:

- Changed display Emulation help text string.
- Removed the Memory subpage from the Performance page.
- Updated GOP setting to (CH)(GOP)0522_ENHPD_DISTURBO_T15T16_RVB_HPD_DIS.bin
- Updated VBIOS to (CH)(VBIOS)0729_ENHPD_DISTURBO_T15T16_3D_HPD_DIS.dat for disable HPD pin.
- Updated boot-up behavior from a G3 state (completely off).
- Added check for memory validation in BIOS library.
- Fixed BIOS code for security fixes.
- Blocked /reboot and /shutdown commands when running AFU tool.

BIOS Version 0035 - CHAPLCEL.0035.2019.0902.1916

About This Release:

- Date: September 2, 2019
- ROM Image Checksum: 0xA8B5
- TXE Firmware: 3.1.70.2331
- PMC Firmware: 03.1F
- EC1 Firmware: 0D.19.00
- EC2 Firmware: 0D.19.00
- Framework Reference Code: Based on 1.4.6
- LAN Option ROM: i211 GbE
- Visual BIOS: AMI
- Supported Flash Devices:

Win Bond	W25Q128FWSIQ	16 MB (1.8V)
GD	GD25LB128DSIGR	16 MB (1.8V)
MACRONIX	MX25U12873FM2I-10G	16 MB (1.8V)

- Microcode Updates included in .BIN & .CAP Files:
  M03506C9_0000003C.PDB

New Fixes/Features:

- Updated CPU microcode to M03506C9_0000003C.PDB.

- Set User Access Level for USB Port Host/Device Mode.

BIOS Version 0032 - CHAPLCEL.0032.2019.0812.2035

About This Release:

- Date: August 12, 2019
- ROM Image Checksum: 0xD1D7
- TXE Firmware: 3.1.70.2331
- PMC Firmware: 03.1F
- EC1 Firmware: 0D.19.00
- EC2 Firmware: 0D.19.00
- Framework Reference Code: Based on 1.4.6
- LAN Option ROM: None
- Supported Flash Devices:

Win Bond	W25Q128FWSIQ	16 MB (1.8V)
GD	GD25LB128DSIGR	16 MB (1.8V)
MACRONIX	MX25U12873FM2I-10G	16 MB (1.8V)

- Microcode Updates included in .ROM File:
  M03506C9_00000036.PDB

New Fixes/Features:

- Initial production BIOS release

LEGAL INFORMATION