BIOS Update Release Notes

PRODUCTS: NUC8i3PNB, NUC8i3PNK, NUC8i3PNH

BIOS Version 0042 - PNWHL357.0042.2021.0505.1525

About This Release:

- Date: May 05, 2021
- ROM Image Checksum: A6CCC8D0
- ME Firmware: 12.0.81.1753
- EC Firmware: 00.40.00
- EC2 Firmware: 0.20
- PD Firmware: 1.5.06
- Memory Reference Code: Based on 7.0.68.40
- MEBx Revision: 12.0.0.0010
- Integrated Graphics:
  - VBIOS: 9.2.1020
  - GOP: 9.0.1085
- AHCI Code: Based on AHCI_19
- LAN Option ROM: 0.5
- Visual BIOS: Intel AptioV

- Supported Flash Devices:
  - Macronix MX25L25673 32MB

- Microcode Updates included in .BIN & .CAP Files:
  - MD0806EB_000000EA.pdb
  - M94806EC_000000EA.pdb

New Fixes/Features:

- Updated ME Firmware to 12.0.81.1753
- Updated EC Firmware to 00.40.00
- Updated EC2 Firmware to 0.20
- Fixed issue where system would reboot when pressing power button in the BIOS setup menu.
- Fixed issue where system could not see logo when booting.
- Updated NTFS DXE driver when parsing NTFS file system partition.
- Fixed issue with virtual display on HDMI_1 port (EC2), it did not get recognized.
- Fixed SMI handler vulnerabilities.
- Added protection code for unauthorized write at controllable address in SMRAM.
- Updated BIOS code for security fixes.

Known Errata:

- Due to the Intel® ME firmware update in BIOS version 0042, you can’t downgrade to version 0041 or earlier.

BIOS Version 0041 - PNWHL357.0041.2020.1209.1904

About This Release:

- Date: December 09, 2020
- ROM Image Checksum: A6482FE9
- ME Firmware: 12.0.71.1681
- EC Firmware: 00.39.00
- EC2 Firmware: 0.19
- PD Firmware: 1.5.06
- Memory Reference Code: Based on 7.0.68.40
- MEBx Revision: 12.0.0.0010
- Integrated Graphics:
  - VBIOS: 9.2.1020

- GOP: 9.0.1085
- AHCI Code: Based on AHCI_19
- LAN Option ROM: 0.5
- Visual BIOS: Intel AptioV

- Supported Flash Devices:
  - Macronix MX25L25673   32MB

- Microcode Updates included in .BIN & .CAP Files:
  - MD0806EB_000000DE.pdb
  - M94806EC_000000DE.pdb

New Fixes/Features:
- Updated ME Firmware 12.0.71.1681
- Updated BIOS code for security fixes

Known Errata:
- **User is required to use transition BIOS PN0040 before flashing to this release due to ME firmware BIOS layout change.**

BIOS Version 0040 - PNWHL357.0040.2020.1201.1834

About This Release:
- Date: December 01, 2020
- ROM Image Checksum: A673A77B
- ME Firmware: 12.0.45.1509
- EC Firmware: 00.39.00
- EC2 Firmware: 0.19
- PD Firmware: 1.5.06
- Memory Reference Code: Based on 7.0.68.40
- MEBx Revision: 12.0.0.0010
- Integrated Graphics:
  - VBIOS: 9.2.1020
  - GOP: 9.0.1085
- AHCI Code: Based on AHCI_19
- LAN Option ROM: 0.5
- Visual BIOS: Intel AptioV

- Supported Flash Devices:
  - Macronix MX25L25673   32MB

- Microcode Updates included in .BIN & .CAP Files:
  - MD0806EB_000000B8.mcb
  - M94806EC_000000CA.mcb

New Fixes/Features:
- Updated EC Firmware to 00.39.00
- Updated EC2 Firmware to 00.19
- Fixed issue when updating ME Firmware.
- Updated BIOS code for security fixes.
- Added EC WDT (Watchdog Timer) function.

BIOS Version 0039 - PNWHL357.0039.2020.0722.1516

About This Release:
- Date: Jul 22, 2020
- ROM Image Checksum: f6c2a1cc
- ME Firmware: 12.0.45.1509
- EC Firmware: 00.36.00
- EC2 Firmware: 0.17
- PD Firmware: 1.5.06
- Memory Reference Code: Based on 7.0.68.40
- MEBx Revision: 12.0.0.0010
- Integrated Graphics:
  - VBIOS: 9.2.1020

    - GOP: 9.0.1085
- AHCI Code: Based on AHCI_19
- LAN Option ROM: 0.5
- Visual BIOS: Intel AptioV

- Supported Flash Devices:
    - Macronix MX25L25673   32MB

- Microcode Updates included in .BIN & .CAP Files:
    - MD0806EB_000000B8.mcb
    - M94806EC_000000CA.mcb

New Fixes/Features:
- Updated EC Firmware to 00.36.00
- Updated EC2 Firmware to 0.17
- Added additional feature for VR current limit.
- Fixed BIOS watchdog counter not clearing.
- Disabled BIOS Self Recovery when Failsafe Watchdog is disabled
- Fixed issue with Thunderbolt Boot default setting. Changed from enabled to disabled by every BIOS flash method.

BIOS Version 0037 - PNWHL357.0037.2020.0324.1446

About This Release:
- Date: Mar 24, 2020
- ROM Image Checksum: 0e1b
- ME Firmware: 12.0.45.1509
- EC Firmware: 00.34.00
- EC2 Firmware: 0.16
- PD Firmware: 1.5.06
- Memory Reference Code: Based on 7.0.68.40
- MEBx Revision: 12.0.0.0010
- Integrated Graphics:
    - VBIOS: 9.2.1020
    - GOP: 9.0.1085
- AHCI Code: Based on AHCI_19
- LAN Option ROM: 0.5
- Visual BIOS: Intel AptioV

- Supported Flash Devices:
    - Macronix MX25L25673   32MB

- Microcode Updates included in .BIN & .CAP Files:
    - MD0806EB_000000B8.mcb
    - M94806EC_000000CA.mcb

New Fixes/Features:
- Updated EC FW to 00.34.00
- Fixed issue where missing variable lock allowed write data to SMRAM.
- Fixed issue where USB 2.0 device in internal USB 3.0 port does not display remove icon.
- Added "Internal USB Port as exposed USB port" setup item.
- Fixed issue not showing Energy Star logo.
- Fixed issue where actual panel brightness would not change after adjust Screen Brightness item in BIOS Setup->Advanced->Flat Panel with eDP panel connect.
- Fixed issue where eDP option still lists in IGD Primary Video Port while no eDP Panel connect.
- Fixed issue where iSetupCfg did not generate full list of UQI values.

BIOS Version 0032 - PNWHL357.0032.2019.1213.1541

About This Release:

- Date: Dec 13, 2019
- ROM Image Checksum: C7AA
- ME Firmware: 12.0.45.1509
- EC Firmware: 00.29.00
- EC2 Firmware: 0.14
- PD Firmware: 1.5.06
- Memory Reference Code: Based on 7.0.68.40
- MEBx Revision: 12.0.0.0010
- Integrated Graphics:
  - VBIOS: 9.2.1020
  - GOP: 9.0.1085
- AHCI Code: Based on AHCI_19
- LAN Option ROM: 0.5
- Visual BIOS: Intel AptioV

- Supported Flash Devices:
  Macronix MX25L25673   32MB

- Microcode Updates included in .BIN & .CAP Files:
  MD0806EB_000000B8.mcb
  M94806EC_000000CA.mcb

New Fixes/Features:

- Initial production BIOS release