BIOS Update Release Notes

PRODUCTS: NUC8i7INH, NUC8i5INH

BIOS Version 0041 - INWHL357.0041.2021.0428.1543

About This Release:

- Date: April 28, 2021
- ROM Image Checksum: 0xAF 4823EE
- ME Firmware: 12.0.72.1757
- EC Firmware: 18.00
- Memory Reference Code: Based on 7.0.5E.40
- Intel RST Pre-OS:
  - UEFI Driver: 17.2.5.4046
  - Legacy Option ROM: 17.2.5.4046
- AHCI Code: Based on AHCI_19
- Wired LAN Adapter:
  - Option ROM: 0.1.13
  - Gbe NVM: v0.5
- Visual BIOS: Intel AptioV

- Supported Flash Devices:
  WinBond W25Q128JVSIQ 16MB

- Microcode Updates included in .BIN & .CAP Files:
  MD0806EB_000000EA.pdb
  M94806EC_000000EA.pdb
  M2240671_0000001E.mcb

New Fixes/Features:

- Updated NTFS DXE driver when parsing NTFS file system partition.
- Updated CPU Microcode MD0806EB_000000EA.pdb and M94806EC_000000EA.pdb
- Fixed OFBD module SMI handler vulnerabilities.
- Added protection code for unauthorized write at controllable address in SMRAM.
- Fixed issue to achieve arbitrary write in SMRAM save state region.

BIOS Version 0040 - INWHL357.0040.2021.0225.1025

About This Release:

- Date: February 25, 2021
- ROM Image Checksum: 0xAF 55477A
- ME Firmware: 12.0.72.1757
- EC Firmware: 18.00
- Memory Reference Code: Based on 7.0.5E.40
- Intel RST Pre-OS:
  - UEFI Driver: 17.2.5.4046
  - Legacy Option ROM: 17.2.5.4046
- AHCI Code: Based on AHCI_19
- Wired LAN Adapter:
  - Option ROM: 0.1.13
  - Gbe NVM: v0.5
- Visual BIOS: Intel AptioV

- Supported Flash Devices:
  WinBond W25Q128JVSIQ 16MB

- Microcode Updates included in .BIN & .CAP Files:
  MD0806EB_000000DE.pdb
  M94806EC_000000DE.pdb
  M2240671_0000001E.mcb

New Fixes/Features:

- Improved BIOS code.
- Updated ME Firmware to 12.0.72.1757

BIOS Version 0039 - INWHL357.0039.2020.1112.1133

About This Release:

- Date: November 11, 2020
- ROM Image Checksum: 0xAF 562B6D
- ME Firmware: 12.0.71.1681
- EC Firmware: 18.00
- Memory Reference Code: Based on 7.0.5E.40
- Intel RST Pre-OS:
  - UEFI Driver: 17.2.5.4046
  - Legacy Option ROM: 17.2.5.4046
- AHCI Code: Based on AHCI_19
- Wired LAN Adapter:
  - Option ROM: 0.1.13
  - Gbe NVM: v0.5
- Visual BIOS: Intel AptioV

- Supported Flash Devices:
  WinBond W25Q128JVSIQ 16MB

- Microcode Updates included in .BIN & .CAP Files:
  MD0806EB_000000DE.pdb
  M94806EC_000000DE.pdb
  M2240671_0000001E.mcb

New Fixes/Features:

- ME firmware update 12.0.71.1681
- Updated BIOS code for security fixes.

BIOS Version 0038 - INWHL357.0038.2020.0701.1702

About This Release:

- Date: July 01, 2020
- ROM Image Checksum: 0xAF 756F41
- ME Firmware: 12.0.49.1534
- EC Firmware: 18.00
- Memory Reference Code: Based on 7.0.5E.40
- Intel RST Pre-OS:
  - UEFI Driver: 17.2.5.4046
  - Legacy Option ROM: 17.2.5.4046
- AHCI Code: Based on AHCI_19
- Wired LAN Adapter:
  - Option ROM: 0.1.13
  - Gbe NVM: v0.5
- Visual BIOS: Intel AptioV

- Supported Flash Devices:

WinBond W25Q128JVSIQ 16MB

- Microcode Updates included in .BIN & .CAP Files:
  MD0806EB_000000CA.pdb
  M94806EC_000000CA.pdb
  M2240671_0000001E.mcb

New Fixes/Features:

- Fixed issue where attempting to update NUC BIOS bricked the system.
- Updated BIOS code for security fixes.

BIOS Version 0036 - INWHL357.0036.2019.1205.1550

About This Release:

- Date: Dec 05, 2019
- ROM Image Checksum: 0xE67D
- ME Firmware: 12.0.49.1534
- EC Firmware: 18.00
- Memory Reference Code: Based on 7.0.5E.40
- Intel RST Pre-OS:
  - UEFI Driver: 17.2.5.4046
  - Legacy Option ROM: 17.2.5.4046
- AHCI Code: Based on AHCI_19
- Wired LAN Adapter:
  - Option ROM: 0.1.13
  - Gbe NVM: v0.5
- Visual BIOS: Intel AptioV

- Supported Flash Devices:
  WinBond W25Q128JVSIQ 16MB

- Microcode Updates included in .BIN & .CAP Files:
  MD0806EB_000000B8.mcb
  M94806EC_000000B8.mcb

New Fixes/Features:

- Updated ME Firmware to 12.0.49.1534.
- Fixed Intel DMI Tool issue.

BIOS Version 0035 - INWHL357.0035.2019.1021.1806

About This Release:

- Date: October 21, 2019
- ROM Image Checksum: 0xB735
- ME Firmware: 12.0.33.1424
- EC Firmware: 18.00
- Memory Reference Code: Based on 7.0.5E.40
- Intel RST Pre-OS:
  - UEFI Driver: 17.2.5.4046
  - Legacy Option ROM: 17.2.5.4046
- AHCI Code: Based on AHCI_19
- Wired LAN Adapter:
  - Option ROM: 0.1.13
  - Gbe NVM: v0.5
- Visual BIOS: Intel AptioV
- Supported Flash Devices:
  WinBond W25Q128JVSIQ 16MB
- Microcode Updates included in .BIN & .CAP Files:
  MD0806EB_000000B8.mcbs

M94806EC_000000B8.mcb

New Fixes/Features:

- Changed the SMBIOS Field "Family name" default to "IN".

BIOS Version 0034 - INWHL357.0034.2019.1002.1952

About This Release:

- Date: October 2, 2019
- ROM Image Checksum: 0x16E5
- ME Firmware: 12.0.33.1424
- EC Firmware: 18.00
- Memory Reference Code: Based on 7.0.5E.40
- Integrated Graphics
  - Option ROM: NA
  - UEFI Driver: NA
- Intel RST Pre-OS:
  - UEFI Driver: 17.2.5.4046
  - Legacy Option ROM: 17.2.5.4046
- External SATA Option ROM: NA
- AHCI Code: Based on AHCI_19
- Wired LAN Adapter:
  - Option ROM: 0.1.13
  - Gbe NVM: v0.5
- Supported Flash Devices:
  WinBond W25Q128JVSIQ 16MB
- Microcode Updates included in .ROM File:
  MD0806EB_000000B8.mcbs
  M94806EC_000000B8.mcb
- Additional Microcode Updates included only in .BIO File:
  MD0806EB_000000B8.mcb
  M94806EC_000000B8.mcb

New Fixes/Features:

- Updated BIOS code for security fixes.
- Implemented SMBIOS field update.
- Updated BIOS to support OAID command

BIOS Version 0033 - INWHL357.0033.2019.0823.1431

About This Release:

- Date: August 23, 2019
- ROM Image Checksum: 0xD7E7
- ME Firmware: 12.0.33.1424
- EC Firmware: 18.00
- Memory Reference Code: Based on 7.0.5E.40
- Intel RST Pre-OS:
  - UEFI Driver: 17.2.5.4046
  - Legacy Option ROM: 17.2.5.4046
- AHCI Code: Based on AHCI_19
- Wired LAN Adapter:
  - Option ROM: 0.1.13
  - Gbe NVM: v0.5
- Visual BIOS: Intel AptioV
- Supported Flash Devices:
  - WinBond W25Q128JVSIQ 16MB
- Microcode Updates included in .BIN & .CAP Files:
  - MD0806EB_000000B8.mcb

- M94806EC_000000B8.mcb

New Fixes/Features:

- Improved BIOS code.

Known Errata

- Due to a security enhancement and ME firmware update in BIOS version 0032, you will not be able to downgrade the BIOS to any version earlier than 0032.

BIOS Version 0032 - INWHL357.0032.2019.0531.1516

About This Release:

- Date: May 31, 2019
- ME Firmware: 12.0.33.1424
- EC Firmware: 18.00
- PMC Firmware: 300.1.20.1023
- Memory Reference Code: Based on 7.0.5E.40
- Intel RST Pre-OS:
  - UEFI Driver: 17.2.5.4046
  - Legacy Option ROM: 17.2.5.4046
- AHCI Code: Based on AHCI_19
- Wired LAN Adapter:
  - Option ROM: 0.1.13
  - Gbe NVM: v0.5
- Visual BIOS: AptioV

New Fixes/Features:

- Fixed issue: Waking the system from S5 would fail.
- Fixed issue: BIOS defaults wouldn’t load correctly on some options when pressing F9 in BIOS setup.
- Updated: ME firmware to version 12.0.33.1424.
- Updated: RST PreOS firmware to version 17.2.5.4046.
- Fixed issue: Legacy USB support wouldn’t save settings.

Known Errata

- Due to a security enhancement and ME firmware update in BIOS version 0032, you will not be able to downgrade the BIOS to any version earlier than 0032.

BIOS Version 0028 - INWHL357.0028.2019.0408.2051

About This Release:

- Date: April 30, 2019
- ROM Image Checksum: 12ca
- ME Firmware: 12.0.32.1421
- EC Firmware: v18.00
- PMC Firmware: v300.1.20.7023
- Boot Guard ACM: 4351
- Memory Reference Code: Based on 7.0.51.41
- Intel RST Pre-OS:
  - UEFI Driver: 17.2.0.3790
  - Legacy Option ROM: 17.2.0.3790
- AHCI Code: Based on AHCI_19
- Wired LAN Adapter:
  - Option ROM: 0.1.13
  - Gbe NVM: v0.5

New Fixes/Features:

- Initial production BIOS release

LEGAL INFORMATION