BIOS Update Release Notes

PRODUCTS: NUC8i7HVK, NUC8i7HVKVA, NUC8i7HVKVAW, NUC8i7HNK, NUC8i7HNKQC

BIOS Version 0067 - HNKBLi70.86A.0067.2021.0526.1723

About This Release:

- Date: May 26, 2021
- ROM Image Checksum: 0x44E6, 0xA37F (NOBG)
- ME Firmware: 11.8.86.3909
- EC Firmware: 0E.0B.00
- Memory Reference Code: Based on 3.2.0
- Integrated Graphics:
    - Option ROM: 9.0.1051
    - UEFI Driver: 9.0.1074
- SATA RAID Option ROM: 15.9.0.1015
- AHCI Code: Based on AHCI_14
- LAN Option ROM: 7.5.11 i219, 0.0.17 i211
- Visual BIOS: 2.2.25

- Supported Flash Devices:
    - WinBond W25Q128JVSIQ 16MB
    - MACRONIX MX25L12850F 16MB
    - GigaDevice GD25B127D 16MB

- Microcode Updates included in .ROM & .BIO Files:
    - M2A906E9_000000EA.pdb

New Fixes/Features:

- Updated ME Firmware to 11.8.86.3909
- Fixed booting issues with Seagate Firecuda 520 SSD type.
- Updated OFBD module SMI handler vulnerabilities.
- Added protection code for unauthorized write at controllable address in SMRAM.
- Updated CPU Microcode to M2A906E9_000000EA.pdb
- Fixed issue to achieve arbitrary write in SMRAM save state region.

Known Errata:

- Due to the Intel® ME firmware update in BIOS version 0067, you cannot downgrade to version 0066 or earlier.

BIOS Version 0066 - HNKBLi70.86A.0066.2021.0310.1823

About This Release:

- Date: Mar 10, 2021

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

- ROM Image Checksum: 0xB46E, 0x1307 (NOBG)
- ME Firmware: 11.8.83.3874
- EC Firmware: 0E.0B.00 (11.00)
- Memory Reference Code: Based on 3.2.0
- Integrated Graphics:
  - Option ROM: 9.0.1051
  - UEFI Driver: 9.0.1074
- SATA RAID Option ROM: 15.9.0.1015
- AHCI Code: Based on AHCI_14
- LAN Option ROM: 7.5.11 i219, 0.0.17 i211
- Visual BIOS: 2.2.25

- Supported Flash Devices:
  - WinBond W25Q128JVSIQ 16MB
  - MACRONIX MX25L12850F 16MB
  - GigaDevice GD25B127D 16MB

- Microcode Updates included in .ROM & .BIO Files:
  - M2A906E9_000000DE.pdb

New Fixes/Features:
- Updated: ME FW version to 11.8.83.3874.
- Security enhancements.
- Updated: EC FW to 0E.0B.00 (11.00)
- Fixed: LEDs (front and skull) no longer work in S0 after updating to BIOS 0064.[+]

Known Errata:
- Due to the Intel® ME firmware update in BIOS version 0066, you cannot downgrade to version 0065 or earlier.

[+]After loading the BIOS, make sure to load the BIOS defaults, save and restart, otherwise the lights may not work.

BIOS Version 0065 - HNKBLi70.86A.0065.2021.0113.1340

About This Release:
- Date: Jan 13, 2021
- ROM Image Checksum: 0x3BBA, 0x9A53 (NOBG)
- ME Firmware: 11.8.82.3838
- EC Firmware: 0E.0A.00
- Memory Reference Code: Based on 3.2.0
- Integrated Graphics:
  - Option ROM: 9.0.1051
  - UEFI Driver: 9.0.1074
- SATA RAID Option ROM: 15.9.0.1015
- AHCI Code: Based on AHCI_14
- LAN Option ROM: 7.5.11 i219, 0.0.17 i211
- Visual BIOS: 2.2.25

- Supported Flash Devices:
  WinBond W25Q128JVSIQ 16MB

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

MACRONIX MX25L12850F 16MB
GigaDevice GD25B127D 16MB

- Microcode Updates included in .ROM & .BIO Files:
  M2A906E9_000000DE.pdb

New Fixes/Features:

- Update ME Firmware version to 11.8.82.3838

Known Errata:

- Due to the Intel® ME firmware update in BIOS version 0065, you can't downgrade to version 0064 or earlier.

BIOS Version 0064 - HNKBLi70.86A.0064.2020.1028.1438

About This Release:

- Date: Oct 28, 2020
- ROM Image Checksum: 0x6D44, 0xCBDD (NOBG)
- ME Firmware: 11.8.80.3746
- EC Firmware: 0E.0A.00
- Memory Reference Code: Based on 3.2.0
- Integrated Graphics:
  - Option ROM: 9.0.1051
  - UEFI Driver: 9.0.1074
- SATA RAID Option ROM: 16.0.2.3402
- AHCI Code: Based on AHCI_14
- LAN Option ROM:
  - i219: 7.5.11
  - i211: 0.0.17
- Visual BIOS: 2.2.25

- Supported Flash Devices:
  WinBond W25Q128JVSIQ 16MB
  MACRONIX MX25L12850F 16MB
  GigaDevice GD25B127D 16MB

- Microcode Updates included in .ROM & .BIO Files:
  M2A906E9_000000DE.pdb

New Fixes/Features:

- Updated ME firmware to 11.8.80.3746.
- Fixed issue where front USB 3.0 port could not be used.
- Fixed issue where previously programmed NVMe M.2 SSD Admin password showed as "NOT INSTALLED" in Visual BIOS.
- Fixed with analog audio output sample rate support.
- Fixed issue where "SATA M.2 SSD type not displayed in SATA section under Visual BIOS DEVICE".
- Fixed issue where Blue USB ports were powered up while system remained unpowered.
- Fixed issue with arbitrary code execution at PEI phase (WakeUpType).
- Fixed issue where SMRAM overwritten with arbitrary data (microcodeUpdate).

Known Errata:

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

- Due to the Intel® ME firmware update in BIOS version 0064, you can't downgrade to version 0063 or earlier.

BIOS Version 0063 - HNKBLi70.86A.0063.2020.0827.1309

About This Release:

- Date: Aug 27, 2020
- ROM Image Checksum: 0x6AE8, 0x4CFD (NOBG)
- ME Firmware: 11.8.79.3722
- EC Firmware: 0E.09.00
- Memory Reference Code: Based on 3.2.0
- Integrated Graphics:
  - Option ROM: 9.0.1051
  - UEFI Driver: 9.0.1074
- SATA RAID Option ROM: 16.0.2.3402
- AHCI Code: Based on AHCI_14
- LAN Option ROM: 7.5.11 i219, 0.0.17 i211
- Visual BIOS: 2.2.25

- Supported Flash Devices:

WinBond	W25Q128JVSIQ	16MB
MACRONIX	MX25L12850F	16MB
GigaDevice	GD25B127D	16MB

- Microcode Updates included in .ROM & .BIO Files:
  M2A906E9_000000D6.mcb

New Fixes/Features:

- Updated ME FW version to 11.8.79.3722
- Updated BIOS code for security fixes.
- Fixed issue where "Native ACPI OS PCIe Support can't be enabled in BIOS if Thunderbolt Controller is enabled".
- Fixed issue with SGX driver v2.7.101.2 causing "System BSoD during restart Windows 10 20H1 (2004)".
- Fixed issue to able to read storage Admin Passwords created using older BIOS versions.
- Added feature to be able to set BIOS passwords on (2) storage units installed independently.
- Fixed issue when S4/S5 settings were not saved in BIOS.
- Fixed issue where "Set default Family Name" for Microsoft request.
- Fixed issue to display "Energy star logo".
- Fixed issue to display "Press F12 for network service boot" in UEFI.

Known Errata:

- Due to the Intel® ME firmware update in BIOS version 0063, you can't downgrade to version 0059 or earlier.

BIOS Version 0059 - HNKBLi70.86A.0059.2019.1112.1124

About This Release:

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

- Date: Nov 12, 2019
- ROM Image Checksum: 0x03BE, 0xE770(NoBG)
- ME Firmware: 11.8.60.3561
- EC Firmware: 0E.09.00
- Memory Reference Code: Based on 3.2.0
- Integrated Graphics:
  - Option ROM: 9.0.1051
  - UEFI Driver: 9.0.1074
- SATA RAID Option ROM: 16.0.2.3402
- AHCI Code: Based on AHCI_14
- LAN Option ROM: 7.5.11 i219, 0.0.17 i211
- Visual BIOS: 2.2.25
- Supported Flash Devices:
  - WinBond W25Q128JVSIQ 16MB
  - MACRONIX MX25L12850F 16MB
  - GigaDevice GD25B127D 16MB
- Microcode Updates included in .ROM & .BIO Files:
  - M2A906E9_000000B4.mcb

New Fixes/Features:

- Fixed issue where WHQL USB3 Termination test fails.
- Fixed issue with Energy Star Logo.
- Fixed issue where "SMBIOS Field update BIOS" for Microsoft request.
- Fixed issue where "Chassis value type changed during flash by BIO" for Microsoft request
- Improved Hybrid BIOS USB BIOS Recovery code.
- Implemented security fixes.

BIOS Version 0058 - HNKBLi70.86A.0058.2019.0705.1646

About This Release:

- Date: July 05, 2019
- ROM Image Checksum: 0x9377, 0x7729(NOBG)
- ME Firmware: 11.8.60.3561
- EC Firmware: 0E.09.00
- Memory Reference Code: Based on 3.2.0
- Integrated Graphics:
  - Option ROM: 9.0.1051
  - UEFI Driver: 9.0.1074
- SATA RAID Option ROM: 16.0.2.3402
- AHCI Code: Based on AHCI_14
- LAN Option ROM: 7.5.11 i219, 0.0.17 i211
- Visual BIOS: 2.2.25
- Supported Flash Devices:
  - WinBond W25Q128JVSIQ 16MB
  - MACRONIX MX25L12850F 16MB
  - GigaDevice GD25B127D 16MB
- Microcode Updates included in .ROM & .BIO Files:
  - M2A906E9_000000B4.mcb

New Fixes/Features:

- Fixed issue: Where the TPM disappears from Windows after power loss.

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

- Fixed issue: Where the power button never turns orange when using the Power Button Recovery process.
- Updated BIOS code for security fixes.

BIOS Version 0057 - HNKBLi70.86A.0057.2019.0528.1518

About This Release:

- Date: May 28, 2019
- ROM Image Checksum: 0xDBAD, 0xBF5F(NOBG)
- ME Firmware: 11.8.60.3561
- EC Firmware: 0E.09.00
- Memory Reference Code: Based on 3.2.0
- Integrated Graphics
  - Option ROM: 9.0.1051
  - UEFI Driver: 9.0.1074
- SATA RAID Option ROM: 16.0.2.3402
- AHCI Code: Based on AHCI_14
- LAN Option ROM: 7.5.11 i219, 0.0.17 i211
- Visual BIOS: 2.2.25

New Fixes/Features:

- Updated BIOS code for security fixes.
- Updated Intel® ME firmware to version 11.8.60.3561.

Known Errata:

- Due to the Intel® ME firmware update in BIOS version 0057, you can’t downgrade to version 0056 or earlier.

BIOS Version 0056 - HNKBLi70.86A.0056.2019.0506.1527

About This Release:

- Date: May 6, 2019
- ME Firmware: 11.8.50.3460
- EC Firmware: 0E.09.00
- Memory Reference Code: Based on 3.2.0
- Integrated Graphics
  - Option ROM: 9.0.1051
  - UEFI Driver: 9.0.1074
- SATA RAID Option ROM: 16.0.2.3402
- AHCI Code: Based on AHCI_14
- LAN Option ROM: 7.5.11 i219, 0.0.17 i211
- Visual BIOS: 2.2.25

New Fixes/Features:

- Updated BIOS to display ENERGY STAR logo on Mini PC SKUs.
- Changed enclosure type default to 0x23.

BIOS Version 0054 - HNKBLi70.86A.0054.2019.0214.1350

About This Release:

- Date: February 14, 2019
- ME Firmware: 11.8.50.3460
- EC Firmware: 0E.09.00
- Memory Reference Code: Based on 3.2.0

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

- Integrated Graphics
  - Option ROM: 9.0.1051
  - UEFI Driver: 9.0.1074
- SATA RAID Option ROM: 15.9.0.1015
- AHCI Code: Based on AHCI_14
- LAN Option ROM: 7.5.11 i219, 0.0.17 i211
- Visual BIOS: 2.2.25

New Fixes/Features:

- Updated BIOS code for security fixes.

BIOS Version 0053 - HNKBLi70.86A.0053.2018.1217.1739

About This Release:

- Date: December 17, 2018
- ME Firmware: 11.8.50.3460
- EC Firmware: 0E.09.00
- Memory Reference Code: Based on 3.2.0
- Integrated Graphics
  - Option ROM: 9.0.1051
  - UEFI Driver: 9.0.1074
- SATA RAID Option ROM: 16.0.2.3402
- AHCI Code: Based on AHCI_14
- LAN Option ROM: 7.5.11 i219, 0.0.17 i211
- Visual BIOS: 2.2.25

New Fixes/Features:

- Fixed issue where disk encryption on Samsung eDrive doesn’t work.

BIOS Version 0052 - HNKBLi70.86A.0052.2018.1129.1700

About This Release:

- Date: November 29, 2018
- ME Firmware: 11.8.50.3460
- EC Firmware: 0E.09.00
- Memory Reference Code: Based on 3.2.0
- Integrated Graphics
  - Option ROM: 9.0.1051
  - UEFI Driver: 9.0.1074
- SATA RAID Option ROM: 16.0.2.3402
- AHCI Code: Based on AHCI_14
- LAN Option ROM: 7.5.11 i219, 0.0.17 i211
- Visual BIOS: 2.2.25

New Fixes/Features:

- Modified code to speed up boot time.
- Fixed Intel ME loss when “After Power Failure” is set to Power On.

BIOS Version 0051 - HNKBLi70.86A.0051.2018.1024.1600

About This Release:

- Date: October 24, 2018
- ME Firmware: 11.8.50.3460

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

- EC Firmware: 0E.09.00
- Memory Reference Code: Based on 3.2.0
- Integrated Graphics
  - Option ROM: 9.0.1051
  - UEFI Driver: 9.0.1074
- SATA RAID Option ROM: 16.0.2.3402
- AHCI Code: Based on AHCI_14
- LAN Option ROM: 7.5.11 i219, 0.0.17 i211
- Visual BIOS: 2.2.25

New Fixes/Features:

- Fixed the issue where an error would occur when installing VMware* ESXi versions 6.5 and 6.7.
- Fixed the issue that the Intel NUC NUC8i7HNK wouldn’t allow some Linux distributions to install with Secure Boot turned off.
- Fixed the issue where Windows* Task Manager wouldn’t show memory speed correctly.

BIOS Version 0050 - HNKBLi70.86A.0050.2018.0927.1020

About This Release:

- Date: September 27, 2018
- ME Firmware: 11.8.50.3460
- EC Firmware: 0E.09.00
- Memory Reference Code: Based on 3.2.0
- Integrated Graphics
  - Option ROM: 9.0.1051
  - UEFI Driver: 9.0.1074
- SATA RAID Option ROM: 16.0.2.3402
- AHCI Code: Based on AHCI_14
- LAN Option ROM: 7.5.11 i219, 0.0.17 i211
- Visual BIOS: 2.2.25

New Fixes/Features:

- Fixed issue where LAN boot is set as first boot device.
- Fixed issue where system can’t receive CEC QEvent from EC.
- Fixed issue where system hangs during POST when Fast Boot is enabled and RAID is changed to AHCI mode.
- Updated SMBIOS table structure.

BIOS Version 0049 - HNKBLi70.86A.0049.2018.0801.1601

About This Release:

- Date: August 1, 2018
- ME Firmware: 11.8.50.3460
- EC Firmware: 0E.09.00
- Memory Reference Code: Based on 3.2.0
- Integrated Graphics
  - Option ROM: 9.0.1051
  - UEFI Driver: 9.0.1074
- SATA RAID Option ROM: 16.0.2.3402
- AHCI Code: Based on AHCI_14
- LAN Option ROM: 7.5.11 i219, 0.0.17 i211
- Visual BIOS: 2.2.25

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

New Fixes/Features:

- Added Deep S4/S5 item in BIOS setup.

BIOS Version 0048 - HNKBLi70.86A.0048.2018.0725.1749

About This Release:

- Date: July 25, 2018
- ME Firmware: 11.8.50.3460
- EC Firmware: 0E.09.00
- Memory Reference Code: Based on 3.2.0
- Integrated Graphics:
  - Option ROM: 9.0.1051
  - UEFI Driver: 9.0.1074
- SATA RAID Option ROM: 16.0.2.3402
- AHCI Code: Based on AHCI_14
- LAN Option ROM: 7.5.11 i219, 0.0.17 i211
- Visual BIOS: 2.2.25

New Fixes/Features:

- Removed Intel® Ready Mode Technology code/items in BIOS for Intel security fix.

BIOS Version 0047 - HNKBLi70.86A.0047.2018.0718.1706

About This Release:

- Date: July 18, 2018
- ME Firmware: 11.8.50.3460
- EC Firmware: 0E.09.00
- Memory Reference Code: Based on 3.2.0
- Integrated Graphics:
  - Option ROM: 9.0.1051
  - UEFI Driver: 9.0.1074
- SATA RAID Option ROM: 16.0.2.3402
- AHCI Code: Based on AHCI_14
- LAN Option ROM: 7.5.11 i219, 0.0.17 i211
- Visual BIOS: 2.2.25

New Fixes/Features:

- Updated CPU Microcode (Security Advisory-00115).
- Fixed the issue where updating the BIOS would not work when running some memory modules above 2400 MHz.
- Fixed the issue where the system would not power on correctly when the power cord is pulled and the BIOS option "After Power Failure" is set to either, Last State or Power On.
- Updated EC FW to 0E.09.00

BIOS Version 0044 - HNKBLi70.86A.0044.2018.0615.1726

About This Release:

- Date: June 13, 2018
- ME Firmware: 11.8.50.3460
- EC Firmware: 0E.08.00
- Memory Reference Code: Based on 3.2.0

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

- Integrated Graphics
  - Option ROM: 9.0.1051
  - UEFI Driver: 9.0.1074
- SATA RAID Option ROM: 16.0.2.3402
- AHCI Code: Based on AHCI_14
- LAN Option ROM: 7.5.11 i219, 0.0.17 i211
- Visual BIOS: 2.2.25

New Fixes/Features:

- Updated SATA RAID Option ROM to 16.0.2.3402.
- Changed consumer infrared (CIR) to be disabled by default.
- Fixed the issue where disabling the consumer infrared (CIR) would not disable it.
- Fixed the issue where the management engine would not update.

BIOS Version 0040 - HNKBLi70.86A.0040.2018.0516.1521

About This Release:

- Date: May 16, 2018
- ME Firmware: 11.8.50.3460
- EC Firmware: 0E.08.00
- Memory Reference Code: Based on 3.0.1
- Integrated Graphics:
  - Option ROM: 9.0.1051
  - UEFI Driver: 9.0.1074
- SATA RAID Option ROM: 15.9.0.1015
- AHCI Code: Based on AHCI_14
- LAN Option ROM: 7.5.11 i219, 0.0.17 i211
- Visual BIOS: 2.2.25

New Fixes/Features:

- Fixed the issue where Plextor SSDs would cause the system to hang.
- Updated ME FW to 11.8.50.3460
- Fixed the issue where the power button, skull or the eyes LEDs would work correctly when set to breathing.
- Changed the default S0 behavior frequency to 0 for the power button, skull and the eyes LEDs.

BIOS Version 0037 - HNKBLi70.86A.0037.2018.0423.0910

About This Release:

- Date: April 23, 2018
- ME Firmware: 11.8.50.3434
- EC Firmware: 0E.07.00
- Memory Reference Code: Based on 3.0.1
- Integrated Graphics
  - Option ROM: 9.0.1051
  - UEFI Driver: 9.0.1074
- SATA RAID Option ROM: 15.9.0.1015
- AHCI Code: Based on AHCI_14
- LAN Option ROM: 7.5.11 i219, 0.0.17 i211
- Visual BIOS: 2.2.25

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

New Fixes/Features:

- Fixed the issue where the system would not shutdown successfully.
- Legacy boot has been removed.

BIOS Version 0034 - HNKBLi70.86A.0034.2018.0329.1113

About This Release:

- Date: March 29, 2018
- ME Firmware: 11.8.50.3434
- EC Firmware: 0E.07.00
- Memory Reference Code: Based on 3.0.1
- Integrated Graphics
  - Option ROM: 9.0.1051
  - UEFI Driver: 9.0.1074
- SATA RAID Option ROM: 15.9.0.1015
- AHCI Code: Based on AHCI_14
- LAN Option ROM: 7.5.11 i219, 0.0.17 i211
- Visual BIOS: 2.2.25

New Fixes/Features:

- Initial pre-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.

Intel is a trademark of Intel Corporation in the US and other countries.
Copyright (c) 2015 Intel Corporation.

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