BIOS Update Release Notes

PRODUCTS: NUC7i5DNKE, NUC7i5DNHE, NUC7i5DNBE, and NUC7i5DNKPC

BIOS Version 0080 - DNKBLi5v.86A.0080.2023.0912.1621

About This Release:
- Date: Sept 12, 2023
- ROM Image Checksum: 0xB0ED1D90, 0xB0C47BC7 (No FVME)
- ME Firmware: 11.8.94.4494 (v5.1)
- EC Firmware: 0D.12.00
- Memory Reference Code: Based on 3.6.4
- Integrated Graphics:
  - Option ROM: 9.0.1068
  - UEFI Driver: 9.0.1095
- SATA RAID Option ROM: 16.7.0.3513
- AHCI Code: Based on AHCI_14
- LAN Option ROM: PXE 2.1 Build 092
- Visual BIOS: 2.2.25

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

- Microcode Updates included in .ROM & .BIO Files:
  - MC0806E9_000000F4.mcb
  - MC0806EA_000000F4.mcb

New Fixes/Features/Updates:
- Updated 2023.3 IPU Update.
- Updated 2023.2 IPU Update.
- Updated 2023.1 IPU Update.
- Updated CPU Microcode Updated to MC0806E9_000000F4,MC0806EA_000000F4.
- Fixed issue where OOB RW vulnerability.
- Added SmiFlash related solutions including TOCTOU SmiFlash_v2.
- Fixed issue where Incorrect bound check vulnerability.
- Updated ME FW to 11.8.94.4494 (v5.1).
- Fixed issue where EDK2 vulnerabilities.
- Fixed issue where OpenSSL vulnerabilities.
- Updated Update for UsbRtSmm and UsbS5Wakeup.
- Fixed issue where Heap Buffer Overflow in TCG2MeasurePeImage.
- Updated SmiFlash related solution implementation.
- Added PlatformLang Timeout Variable Access.
- Fixed issue where UEFI Variable access vulnerability.
- Fixed issue where SMM memory corruption vulnerability in SMM driver on select Intel platforms.

*Other names and brands may be claimed as the property of others. Intel Confidential*
• Fixed issue where PEI memory corruption on Server boards and on a majority of NUCs.
• Fixed issue where SmmEntryPoint Underflow vulnerability.
• Updated BlackLotus-SecureBoot DBX.
• Fixed issue where BIOS patch of Boot options overflow handling.
• Fixed issue where The stack buffer overflow vulnerability leads to arbitrary code execution in DXE driver on select Intel platforms.
• Fixed issue where MCU update fails through BIOS flash with HW jumper method from DN0076 to DN0079.
• Fixed issue where The prompted password message windows does not display in the center of the screen.
• Fixed issue where The SMART info window is not displayed in the center of the screen.

Known Errata:
• Bitlocker Recovery will occur after reloading the Secure Boot keys in Visual BIOS since DN0080 has an updated Secure Boot DBX.
• Blocked F7 Flash/EBU downgrade to DN0079 and previous versions due to ME FW update.

BIOS Version 0079 – DNKBLi5v.86A.0079.2023.0223.1019

About This Release:
• Date: FEB 23,2023
• ROM Image Checksum: 0xB0D5B71E
• ME Firmware: 11.8.93.4323
• EC Firmware: 0D.12.00
• Memory Reference Code: Based on 3.6.4
• Integrated Graphics:
  Option ROM: 9.0.1068
  UEFI Driver: 9.0.1095
• SATA RAID Option ROM: 15.7.0.3054
• AHCI Code: Based on AHCI_14
• LAN Option ROM: PXE 2.1 Build 092
• Visual BIOS: 2.2.25

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

• Microcode Updates included in .ROM & .BIO Files:
  MCD0806E9_000000F0.mcb

New Fixes/features/Updates:
• Fixed issue where Information disclosure vulnerability.
• Fixed issue where SDIO_DEV_CONFIGURATION SetVariable NVRAM Corruption.
• Updated UEFI Boot Variables Access.
• Fixed issue where UEFI Variable access vulnerability.
• Fixed issue where POST screen displays no warning message when inserting NG NVMe SSD test with S.M.A.R.T setting enabled.
• Updated ME FW to 11.8.93.4323.
• Updated CPU Microcode to MC0806E9_000000F0.
• UpdatedGD 2022 IPU update: 2022.1/2022.3.

*Other names and brands may be claimed as the property of others. Intel Confidential
Known Errata:
- Due to the Intel® ME firmware update in BIOS version 0077, you can’t downgrade to the earlier version.

BIOS Version 0076 - DNKBLi5v.86A.0076.2022.0817.1457

About This Release:
- Date: Aug 17, 2022
- ROM Image Checksum: 6d9f115b (CRC32)
- ME Firmware: 11.8.90.3987
- EC Firmware: 0D.12.00
- Memory Reference Code: Based on 3.6.4
- MEBx Revision: 11.0.0.0010
- Integrated Graphics:
  - Option ROM: 9.0.1051
  - UEFI Driver: 9.0.1066
- SATA RAID Option ROM: 15.7.0.3054
- AHCI Code: Based on AHCI_14
- LAN Option ROM: PXE 2.1 Build 092
- Visual BIOS: 2.2.25
- Microcode Updates included in .ROM & .BIO Files:
  - MC0806E9_000000EA.mcb

New Fixes/Features:
- Fixed issue where Unauthorized modification of UEFI variables.
- Fixed issue where Unauthorized modification of UEFI variables could disable the protect mechanism of SMM.
- Updated for 2021.2 IPU BIOS change.
- Updated ME FW to 11.8.90.3987 (v9)
- Fixed issue where DN won't flash correctly via power button menu update from 0075 to 0075.

Known Errata:
- Due to the Intel® ME firmware update in BIOS version 0075, you can’t downgrade to earlier version.

BIOS Version 0075 - DNKBLi5v.86A.0075.2021.1014.1327

About This Release:
- Date: Oct 14, 2021
- ROM Image Checksum: 1bac05e8 (CRC32)
- ME Firmware: 11.8.86.3909

*Other names and brands may be claimed as the property of others. Intel Confidential
• EC Firmware: 0D.12.00
• Memory Reference Code: Based on 3.6.4
• MEBx Revision: 11.0.0.0010
• Integrated Graphics:
  o Option ROM: 9.0.1051
  o UEFI Driver: 9.0.1068
• SATA RAID Option ROM: 15.7.0.3054
• AHCI Code: Based on AHCI_14
• LAN Option ROM: PXE 2.1 Build 092
• Visual BIOS: 2.2.25

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

• Microcode Updates included in .ROM & .BIO Files:
  MC0806E9_000000EA.mcb

**New Fixes/Features:**
- Removed change for "ACPI improvement" for "PTK1456 Memory corruption during S3 resume".
- Fixed issue with unauthorized modification of UEFI variables that could overwrite arbitrary SMRAM.

**Known Errata:**
- Due to the Intel® ME firmware update in BIOS version 0073, you can’t downgrade to version 0072 or earlier.

**BIOS Version 0074 - DNKBLi5v.86A.0074.2021.0716.1950**

**About This Release:**
- Date: July 14, 2021
- ROM Image Checksum: (CRC32)
- ME Firmware: 11.8.86.3909
- EC Firmware: 0D.12.00
- Memory Reference Code: Based on 3.6.4
- MEBx Revision: 11.0.0.0010
- Integrated Graphics:
  o Option ROM: 9.0.1051
  o UEFI Driver: 9.0.1066
- SATA RAID Option ROM: 15.7.0.3054
- AHCI Code: Based on AHCI_14
- LAN Option ROM: PXE 2.1 Build 092
- Visual BIOS: 2.2.25

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

• Microcode Updates included in .ROM & .BIO Files:
  o MC0806E9_000000EA.mcb

**New Fixes/Features:**
Updated: CPU Microcode to 0xEA for IPU 2021.1.
Updated: Security Enhancements.
Updated: ACPI improvement for "PTK1456 Memory corruption during S3 resume".
Fixed: Add protection code for unauthorized write at controllable address in SMRAM.

BIOS Version 0073 – DNKBLi5v.86A.0073.2021.0414.1654

About This Release:
Date: Apr 14, 2021
ROM Image Checksum: E82035DA (CRC32)
ME Firmware: 11.8.86.3909
EC Firmware: 0D.12.00
Memory Reference Code: Based on 3.6.4
MEBx Revision: 11.0.0.0010
Integrated Graphics:
  • Option ROM: 9.0.1051
  • UEFI Driver: 9.0.1066
SATA RAID Option ROM: 15.7.0.3054
AHCI Code: Based on AHCI_14
LAN Option ROM: PXE 2.1 Build 092
Visual BIOS: 2.2.25

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

Microcode Updates included in .ROM & .BIO Files:
  MC0806E9_000000DE.mcb

New Fixes/Features:
• Updated ME Firmware to 11.8.86.3909
• Fixed WatchDog Timer issue with Ubuntu Linux.
• Fixed issue with NTFS DXE driver when parsing NTFS file system partition.
• Updated BIOS code for security fixes.

Known Errata:
• Due to the Intel® ME firmware update in BIOS version 0073, you can’t downgrade to version 0072 or earlier.

BIOS Version 0072 – DNKBLi5v.86A.0072.2021.0219.1507

About This Release:
Date: Feb 19, 2021
ROM Image Checksum: 3a1133dd (CRC32)
ME Firmware: 11.8.81.3807
EC Firmware: 0D.12.00
Memory Reference Code: Based on 3.6.4
MEBx Revision: 11.0.0.0010
Integrated Graphics:
  • Option ROM: 9.0.1051
  • UEFI Driver: 9.0.1066

*Other names and brands may be claimed as the property of others. Intel Confidential
• SATA RAID Option ROM: 15.7.0.3054
• AHCI Code: Based on AHCI_14
• LAN Option ROM: PXE 2.1 Build 092
• Visual BIOS: 2.2.25

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

• Microcode Updates included in .ROM & .BIO Files:
  MC0806E9_000000DE.mcb

New Fixes/Features:
• Updated ME firmware to version 11.8.80.3746.
• Updated microcode to MC0806E9_000000DE.
• Updated BIOS code for security fixes.

BIOS Version 0070 - DNKBLi5v.86A. 0070.2020.0924.0958

About This Release:
• Date: September 24, 2020
• ROM Image Checksum: 0x7F85, 0xDDBC (No FVME)
• ME Firmware: 11.8.80.3746
• EC Firmware: 0D.12.00
• Memory Reference Code: Based on 3.6.4
• MEBx Revision: 11.0.0.0010
• Integrated Graphics
  • Option ROM: 9.0.1051
  • UEFI Driver: 9.0.1066
• SATA RAID Option ROM: 15.7.0.3054
• SATA non-RAID Option ROM: NA
• AHCI Code: Based on AHCI_14
• LAN Option ROM: PXE 2.1 Build 092
• Visual BIOS: 2.2.25

• Supported Flash Devices:
  WinBond W25Q128JVSIQ 16MB
  MACRONIX MX25L12850F 16MB
  GigaDevice GD25B127D 16MB
• Microcode Updates included in .ROM File:
  MC0806E9_0000000D6.mcb
• Additional Microcode Updates included only in .BIO File:
  MC0806E9_000000D6.mcb

New Fixes/Features:
• Updated ME firmware to version 11.8.80.3746.
• Updated microcode to MC0806E9_000000DE.
• Updated BIOS code for security fixes.

Known Errata:
• Due to the Intel® ME firmware update in BIOS version 0070, you can’t
downgrade to version 0069 or earlier.
About This Release:

- Date: June 10, 2020
- ROM Image Checksum: 0xB584, 0x430B (No FVME)
- ME Firmware: 11.8.77.3664
- EC Firmware: 0D.12.00
- Memory Reference Code: Based on 3.6.4
- MEBx Revision: 11.0.0.0010
- Integrated Graphics:
  - Option ROM: 9.0.1051
  - UEFI Driver: 9.0.1095
- SATA RAID Option ROM: 15.7.0.3054
- AHCI Code: Based on AHCI_14
- LAN Option ROM: PXE 2.1 Build 092
- Visual BIOS: 2.2.25
- Supported Flash Devices:
  - WinBond W25Q128JVSIQ 16MB
  - MACRONIX MX25L12850F 16MB
  - GigaDevice GD25B127D 16MB
- Microcode Updates included in .ROM & .BIO Files: MC0806E9_00000018.mcb

New Fixes/Features:

- Updated ME Firmware to 11.8.77.3664.
- Fixed issue where custom BIOS from ITK fails to install when unattended BIOS configuration is set to never prompt.
- Updated BIOS code for security fixes.

Known Errata:

- Due to the Intel® ME firmware update in BIOS version 0069, you can’t downgrade to version 0068 or earlier.

About This Release:

- Date: March 12, 2020
- ROM Image Checksum: 0x1961, 0xA6E8 (No FVME)
- ME Firmware: 11.8.70.3626
- EC Firmware: 0D.12.00
- Memory Reference Code: Based on 3.6.4
- MEBx Revision: 11.0.0.0010
- Integrated Graphics:
  - Option ROM: 9.0.1051
  - UEFI Driver: 9.0.1066
- SATA RAID Option ROM: 15.7.0.3054
- AHCI Code: Based on AHCI_14
- LAN Option ROM: PXE 2.1 Build 092
- Visual BIOS: 2.2.25
- Supported Flash Devices:
WinBond W25Q128JVSIQ 16MB  
MACRONIX MX25L12850F 16MB  
GigaDevice GD25B127D 16MB  

- Microcode Updates included in .ROM & .BIO Files:  
  MC0806E9_000000B4.mcb

**New Fixes/Features:**
- Updated BIOS code for security fixes.
- Fixed issues regarding system reboot and system wake up.
- Fixed issue to “Set default Family Name” to “DN”.
- Updated ME Firmware version to 11.8.70.3626.

**Known Errata:**
- Due to the Intel® ME firmware update in BIOS version 0068, you can’t down grade to version 0067 or earlier.

**BIOS Version 0067 – DNKBLi5v.86A.0067.2019.1101.1757**

**About This Release:**
- Date: November 01, 2019  
  ROM Image Checksum: 0xEAB6, 0x7906 (No FVME)  
  ME Firmware: 11.8.65.3590  
  EC Firmware: 0D.12.00  
  Memory Reference Code: Based on 3.6.4  
  MEBx Revision: 11.0.0.0010  
  Integrated Graphics:  
    - Option ROM: 9.0.1051  
    - UEFI Driver: 9.0.1066  
  SATA RAID Option ROM: 15.7.0.3054  
  AHCi Code: Based on AHCi_14  
  LAN Option ROM: PXE 2.1 Build 092  
  Visual BIOS: 2.2.25  
  Supported Flash Devices:  
    WinBond W25Q128JVSIQ 16MB  
    MACRONIX MX25L12850F 16MB  
    GigaDevice GD25B127D 16MB  
- Microcode Updates included in .ROM & .BIO Files:  
  MC0806E9_000000B4.mcb

**New Fixes/Features:**
- Fixed issue where “Hybrid BIOS USB recovery”.  
- Fixed issue where “Chassis value type changed during flash by BIO” for Microsoft request.  
- Fixed issue where “SMBIOS Field update BIOS” for Microsoft request.  
- Implemented security fixes  
- Added support for “EFI ERASE BLOCK Protocol support for Android”.  
- Updated EC to version 12.00.

**BIOS Version 0066 – DNKBLi5v.86A.0066.2019.0710.1158**

**About This Release:**
- Date: July 10, 2019

*Other names and brands may be claimed as the property of others.*
• ROM Image Checksum: 0x0D8D, 0x9BDD (No FVM)
• ME Firmware: 11.8.65.3590
• EC Firmware: 0D.11.00
• Memory Reference Code: Based on 3.6.4
• MEBx Revision: 11.0.0.0010
• Integrated Graphics
  ▪ Option ROM: 9.0.1051
  ▪ UEFI Driver: 9.0.1066
• SATA RAID Option ROM: 15.7.0.3054
• AHCI Code: Based on AHCI_14
• LAN Option ROM: PXE 2.1 Build 092
• Visual BIOS: 2.2.25
• Supported Flash Devices:
  WinBond W25Q128JVSIQ 16MB
  MACRONIX MX25L12850F 16MB
  GigaDevice GD25B127D 16MB
• Microcode Updates included in .ROM File:
  MC0806E9_000000B4.mcb
• Additional Microcode Updates included only in .BIO File:
  MC0806E9_000000B4.mcb

New Fixes/Features:
• Fixed issue where there’s no display when using eDP panel.
• Fixed issue where BIOS password isn’t recognized.
• Modified BIOS code for security fix

---

**BIOS Version 0065 - DNKBLi5v.86A.0065.2019.0611.1413**

**About This Release:**
• Date: June 11, 2019
• ROM Image Checksum: 0x71EB, 0x003B (No FVM)
• ME Firmware: 11.8.65.3590
• EC Firmware: 0D.11.00
• Memory Reference Code: Based on 3.6.4
• MEBx Revision: 11.0.0.0010
• Integrated Graphics
  ▪ Option ROM: 9.0.1051
  ▪ UEFI Driver: 9.0.1066
• SATA RAID Option ROM: 15.7.0.3054
• AHCI Code: Based on AHCI_14
• LAN Option ROM: PXE 2.1 Build 092
• Visual BIOS: 2.2.25
• Supported Flash Devices:
  WinBond W25Q128JVSIQ 16MB
  MACRONIX MX25L12850F 16MB
  GigaDevice GD25B127D 16MB
• Microcode Updates included in .ROM File:
  MC0806E9_000000B4.mcb
• Additional Microcode Updates included only in .BIO File:
  MC0806E9_000000B4.mcb

New Fixes/Features:
• Updated CPU microcode to MC0806E9_000000B4.
• Removed "SW Control" option from "Button LED" item in BIOS Setup.

*Other names and brands may be claimed as the property of others. Intel Confidential*
BIOS Version 0064 - DNKBLi5v.86A.0064.2019.0523.1933

About This Release:
- Date: May 23, 2019
- ROM Image Checksum: 0xFA93, 0x88E3 (No FVME)
- ME Firmware: 11.8.65.3590
- EC Firmware: 0D.11.00
- Memory Reference Code: Based on 3.6.4
- MEBx Revision: 11.0.0.0010
- Integrated Graphics
  - Option ROM: 9.0.1051
  - UEFI Driver: 9.0.1066
- SATA RAID Option ROM: 15.7.0.3054
- AHCI Code: Based on AHCI_14
- LAN Option ROM: PXE 2.1 Build 092
- Visual BIOS: 2.2.25

New Fixes/Features:
- Fixed TPM provision test failure.

BIOS Version 0063 - DNKBLi5v.86A.0063.2019.0503.1714

About This Release:
- Date: May 3, 2019
- ME Firmware: 11.8.65.3590
- EC Firmware: 0D.11.00
- Memory Reference Code: Based on 3.6.4
- MEBx Revision: 11.0.0.0010
- Integrated Graphics
  - Option ROM: 9.0.1051
  - UEFI Driver: 9.0.1066
- SATA RAID Option ROM: 15.7.0.3054
- AHCI Code: Based on AHCI_14
- LAN Option ROM: PXE 2.1 Build 092
- Visual BIOS: 2.2.25

New Fixes/Features:
- Updated Intel ME firmware to version 11.8.65.3590.
- Modified BIOS code for security fixes.
- Changed enclosure type default to 0x23.

Known Errata:
- Due to the Intel® ME firmware update in BIOS version 0063, you can’t downgrade to version 0062 or earlier.

BIOS Version 0062 - DNKBLi5v.86A.0062.2019.0304.1757

About This Release:
- Date: March 4, 2019
- ME Firmware: 11.8.55.3510
- EC Firmware: 0D.11.00
- Memory Reference Code: Based on 3.6.4
- MEBx Revision: 11.0.0.0010
- Integrated Graphics
  - Option ROM: 9.0.1051
  - UEFI Driver: 9.0.1066
- SATA RAID Option ROM: 15.7.0.3054
- AHCI Code: Based on AHCI_14
- LAN Option ROM: PXE 2.1 Build 092
- Visual BIOS: 2.2.25

**New Fixes/Features:**
- Updated processor microcode.
- Fixed issue where system doesn’t resume from S3 properly.
- Fixed issue where there’s no display when using eDP panel.
- Updated BIOS code for security fixes.

**BIOS Version 0060 - DNKBLi5v.86A.0060.2018.1220.1536**

**About This Release:**
- Date: December 20, 2018
- ME Firmware: 11.8.50.3510
- EC Firmware: 0D.11.00
- Memory Reference Code: Based on 3.2.0
- MEBx Revision: 11.0.0.0010
- Integrated Graphics
  - Option ROM: 9.0.1051
  - UEFI Driver: 9.0.1066
- SATA RAID Option ROM: 15.7.0.3054
- AHCI Code: Based on AHCI_14
- LAN Option ROM: PXE 2.1 Build 092
- Visual BIOS: 2.2.25

**New Fixes/Features:**
- Fixed issue where Hyperthreading can’t be disabled using ITK.
- Fixed issue where disk encryption on Samsung eDrive doesn’t work.
- Fixed issue where BIOS update process in Linux hangs on POST code with 48FE.
- Updated EC firmware to version 11.00.

**BIOS Version 0059 - DNKBLi5v.86A.0059.2018.1129.1604**

**About This Release:**
- Date: November 29, 2018
- ME Firmware: 11.8.55.3510
- EC Firmware: 0D.10.00
- Memory Reference Code: Based on 3.2.0
- MEBx Revision: 11.0.0.0010
- Integrated Graphics
  - Option ROM: 9.0.1051
  - UEFI Driver: 9.0.1066
- SATA RAID Option ROM: 15.7.0.3054
- AHCI Code: Based on AHCI_14
- LAN Option ROM: PXE 2.1 Build 092
- Visual BIOS: 2.2.25

*Other names and brands may be claimed as the property of others.*
New Fixes/Features:
• Set PCIe ASPM function to Disabled.

BIOS Version 0058 - DNKBli5v.86A.0058.2018.1115.1501

About This Release:
• Date: November 15, 2018
• ME Firmware: 11.8.55.3510
• EC Firmware: 0D.10.00
• Memory Reference Code: Based on 3.2.0
• MEBx Revision: 11.0.0.0010
• Integrated Graphics
  ▪ Option ROM: 9.0.1051
  ▪ UEFI Driver: 9.0.1066
• SATA RAID Option ROM: 15.7.0.3054
• AHCI Code: Based on AHCI_14
• LAN Option ROM: PXE 2.1 Build 092
• Visual BIOS: 2.2.25

New Fixes/Features:
• Added NVME hard drive string ID.
• Modified BIOS embedded DP setting.

BIOS Version 0057 - DNKBli5v.86A.0057.2018.1030.1638

About This Release:
• Date: October 30, 2018
• ME Firmware: 11.8.55.3510
• EC Firmware: 0D.10.00
• MEBx Revision: 11.0.0.0010
• Integrated Graphics
  ▪ Option ROM: 9.0.1051
  ▪ UEFI Driver: 9.0.1066
• SATA RAID Option ROM: 15.7.0.3054
• AHCI Code: Based on AHCI_14
• LAN Option ROM: PXE 2.1 Build 092
• Visual BIOS: 2.2.25

New Fixes/Features:
• Added USB Host/Device mode switch item in USB Configuration page.
• Improved USB provision item.
• Fixed issue where Persistence Mode can’t be set to default using ITK 6.1.8.

BIOS Version 0056 - DNKBli5v.86A.0056.2018.1003.1621

About This Release:
• Date: October 03, 2018
• ME Firmware: 11.8.55.3510
• EC Firmware: 0D.10.00
• Memory Reference Code: Based on 3.2.0
• MEBx Revision: 11.0.0.0010
• Integrated Graphics

*Other names and brands may be claimed as the property of others.  Intel Confidential
- Option ROM: 9.0.1051
- UEFI Driver: 9.0.1066
- SATA RAID Option ROM: 15.7.0.3054
- AHCI Code: Based on AHCI_14
- LAN Option ROM: PXE 2.1 Build 092
- Visual BIOS: 2.2.25

**New Fixes/Features:**
- BIOS functionality enhancements.

**BIOS Version 0055 – DNKBLi5v.86A.0055.2018.0921.1432**

**About This Release:**
- Date: September 21, 2018
- ME Firmware: 11.8.55.3510
- EC Firmware: 0D.10.00
- Memory Reference Code: Based on 3.2.0
- MEBx Revision: 11.0.0.0010
- Integrated Graphics
  - Option ROM: 9.0.1051
  - UEFI Driver: 9.0.1066
- SATA RAID Option ROM: 15.7.0.3054
- AHCI Code: Based on AHCI_14
- LAN Option ROM: PXE 2.1 Build 092
- Visual BIOS: 2.2.25

**New Fixes/Features:**
- Fixed issue where system won’t boot when NVMe password is enabled then disabled on Intel E6100P SSD.

**BIOS Version 0053 – DNKBLi5v.86A.0053.2018.0903.2245**

**About This Release:**
- Date: September 3, 2018
- ROM Image Checksum: 0x6A9B, 0xFEE9 (No FVME)
- ME Firmware: 11.8.55.3510
- EC Firmware: 0D.10.00
- Memory Reference Code: Based on 3.2.0
- MEBx Revision: 11.0.0.0010
- Integrated Graphics
  - Option ROM: 9.0.1051
  - UEFI Driver: 9.0.1066
- SATA RAID Option ROM: 15.7.0.3054
- AHCI Code: Based on AHCI_14
- LAN Option ROM: PXE 2.1 Build 092
- Visual BIOS: 2.2.25

**New Fixes/Features:**
- Fixed issue where the front panel LED blink code fails if memory is missing.
- Fixed issue with USB after updating BIOS from version 0044 to version 0052 via Jumper recovery.
- Updated Intel® ME firmware to version 11.8.55.3510.
- Updated BIOS Gigabit Ethernet binary to fix SSID issue.
Due to the Intel® ME firmware update in BIOS version 0053, you can’t downgrade to version 0052 or earlier.

### BIOS Version 0052 - DNKBli5v.86A.0052.2018.0808.1335

**About This Release:**
- Date: August 8, 2018
- ME Firmware: 11.8.50.3425
- EC Firmware: 0D.10.00
- Memory Reference Code: Based on 3.2.0
- MEBx Revision: 11.0.0.0010
- Integrated Graphics:
  - Option ROM: 9.0.1051
  - UEFI Driver: 9.0.1066
- SATA RAID Option ROM: 15.7.0.3054
- AHCI Code: Based on AHCI_14
- LAN Option ROM: PXE 2.1 Build 092
- Visual BIOS: 2.2.25

**New Fixes/Features:**
- Fixed the issue that would cause the system not to power on.
- Fixed the issue where M.2 PCIe SSDs would run at Generation 2 speeds. *
- Removed Intel Ready Mode.
- Fixed the issue that would cause the system to automatically wake from S3 when a device was connected to the 3.5mm jack.
- Fixed the issue that would cause the wireless and Bluetooth options to disappear after they were enabled.
- Fixed the issue where “Wake on USB from S5” wouldn’t work (“USB S4/S5 Power must be turned on to see this option).

*To fix the M.2 issue, the BIOS must be installed using the [jumper recovery method](#).*

### BIOS Version 0050 - DNKBli5v.86A.0050.2018.0716.1547

**About This Release:**
- Date: July 16, 2018
- ME Firmware: 11.8.50.3425
- EC Firmware: 0D.10.00
- Memory Reference Code: Based on 3.2.0
- MEBx Revision: 11.0.0.0010
- Integrated Graphics:
  - Option ROM: 9.0.1051
  - UEFI Driver: 9.0.1066
- SATA RAID Option ROM: 15.7.0.3054
- AHCI Code: Based on AHCI_14
- LAN Option ROM: PXE 2.1 Build 092
- Visual BIOS: 2.2.25

**New Fixes/Features:**
- Added the feature to keep USB power during System Reset.
- Fixed the issue where BIOS recovery wouldn’t work.
- Fixed the Wake on LAN from S3 issue where the monitor wouldn’t wake up.

*Other names and brands may be claimed as the property of others.*
BIOS Version 0047 - DNKBLi5v.86A.0047.2018.0613.1739

About This Release:
- Date: June 13, 2018
- ME Firmware: 11.8.50.3425
- EC Firmware: 0D.10.00
- Memory Reference Code: Based on 3.2.0
- MEBx Revision: 11.0.0.0010
- Integrated Graphics
  - Option ROM: 9.0.1051
  - UEFI Driver: 9.0.1066
- SATA RAID Option ROM: 15.7.0.3054
- AHCI Code: Based on AHCI_14
- LAN Option ROM: PXE 2.1 Build 092
- Visual BIOS: 2.2.25

New Fixes/Features:
- Enabled fanless mode.
- Updated the EC to version 10.00
- Fixed the issue where the splash screen logo would be askew in the OS recovery process.
- Improved the fault tolerance when using the recovery process.
- Updated CPU Microcode (Security Advisory-00115)
- Updated the TPM 2.0 security.
- Added TPM FW update functionality.

BIOS Version 0040 - DNKBLi5v.86A.0040.2018.0315.1451

About This Release:
- Date: March 15, 2018
- ME Firmware: 11.8.50.3425
- EC Firmware: 0D.09.00
- Integrated Graphics:
  - Option ROM: 9.0.1051
  - UEFI Driver: 9.0.1066
- SATA RAID Option ROM: 15.7.0.3054
- AHCI Code: Based on AHCI_14
- LAN Option ROM: PXE 2.1 Build 092
- Visual BIOS: 2.2.25

New Fixes/Features:
- Updated EC firmware version to 9.00.
- Implemented emulation option.
- Fixed USB provisioning setting.
- Fixed issue with disabling USB port in M.2 Wireless Slot for Bluetooth.

BIOS Version 0039 - DNKBLi5v.86A.0039.2018.0222.1752

About This Release:
- Date: February 22, 2018
- ME Firmware: 11.8.50.3425
- EC Firmware: 0D.08.00
- Integrated Graphics:
New Fixes/Features:
- Updated CPU Microcode (Security Advisory-00088)

---

**BIOS Version 0037 - DNKBLi5v.86A.0037.2018.0131.1029**

About This Release:
- Date: January 11, 2018
- ME Firmware: 11.8.50.3425
- EC Firmware: 0D.08.00
- MEBx Revision: 11.0.0.0010
- Integrated Graphics
  - Option ROM: 9.0.1051
  - UEFI Driver: 9.0.1066
- SATA RAID Option ROM: 15.7.0.3054
- SATA non-RAID Option ROM: NA
- AHCI Code: Based on AHCI_14
- LAN Option ROM: PXE 2.1 Build 092
- Visual BIOS: 2.2.25

New Fixes/Features:
- Fixed the issue with fan setting changes cannot be retained
- Fixed the issue auto wake from S4 when “wake system from S5” is enabled in bios
- Fixed an error with the OEM Activation Tool.
- Renamed the USB 3.0 setup options for clarity.
- Update EC version to 8.00.
- Update RC version to 3.0.0
- Added the BIOS setup option, “Screen Rotation Policy” to allow the screen orientation to be changed through the BIOS.
- Added the BIOS setup options, “PCIe Port in M.2 Wireless Slot (For WLAN)” and “USB Port in M.2 Wireless Slot (For Bluetooth)” to enable or disable Wireless and/or Bluetooth separately.
- Due to a security enhancement, it will not be possible to go to any BIOS earlier than BIOS DNi5v0037.

---

**BIOS Version 0031 - DNKBLi5v.86A.0031.2017.1123.1612**

About This Release:
- Date: November 23, 2017
- ME Firmware: 11.8.50.3425
- EC Firmware: 0C.06.00
- MEBx Revision: 11.0.0.0010
- Integrated Graphics
  - Option ROM: 9.0.1051
  - UEFI Driver: 9.0.1066
- SATA RAID Option ROM: 15.7.0.3054
- AHCI Code: Based on AHCI_14

*Other names and brands may be claimed as the property of others.*
• LAN Option ROM: PXE 2.1 Build 092
• Visual BIOS: 2.2.25

New Fixes/Features:
• Changed default setting for “IGD Flat Panel” to enabled.
• Changed the BIOS option “USB Host/Device Mode” to “USB 3.0 Port Header Configuration”.
• Added the BIOS option to turn USB power off and on.
• Updated Management Engine Firmware to version: 11.8.50.3425 (Security Advisory-00086).
• Initial units of NUC7i5DNxE with the SA# -502 and -503 need to be updated to BIOS release 0031 or later in order for Intel Unite® to work.


About This Release:
• Date: September 15, 2017
• ME Firmware: 11.7.0.3307
• EC Firmware: 0C.06.00
• MEBx Revision: 11.0.0.0010
• Integrated Graphics
  o Option ROM: 9.0.1051
  o UEFI Driver: 9.0.1066
• SATA RAID Option ROM: 15.7.0.3054
• AHCI Code: Based on AHCI_14
• LAN Option ROM: PXE 2.1 Build 092
• Visual BIOS: 2.2.25

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, lifesaving, 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) 2021 Intel Corporation.

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