



BIOS Update Release Notes

PRODUCTS: NUC8i7BEH, NUC8i5BEH, NUC8i5BEK, NUC8i3BEH, NUC8i3BEK, NUC8i7BEHGA, NUC8i7BEKQA, NUC8i5BEHFA, NUC8i5BEKPA, NUC8i3BEHFA

BIOS Version 0095 - BECFL357.86A.0095.2023.0918.1953

About This Release:

- Date: Sept 18, 2023
- ROM Image Checksum: 0x8C20
- EC Firmware: v3.26
- ME Firmware: 12.0.93.2331
- PMC Firmware: 300.1.20.1030
- I219 NVM: 0.4
- CRB Label: 1AUOK034
- Boot Guard ACM: 1.8.0
- Bios Guard: Based on BiosGuard_056
- Silicon initialization Code: Based on 7.0.51.41
- Memory Reference Code: 0,7,1,95
- Integrated Graphics:
 - Option ROM: v1026
 - UEFI Driver: v9.0.1098
- SATA RAID Option ROM: 17.8.0.4507
- AHCI Code: Based on AHCI_19
- LAN Option ROM: PXE V0.1.1.3
- Visual BIOS: 2.2.23
- Supported Flash Devices:

WinBond	W25Q128JVS1Q	16MB (3.3V)
Macronix	MX25L12873FM2I-10G	16MB (3.3V)
GigaDevice	GD25B127DSIGR	16MB (3.3V)
- Microcode Updates included in .ROM & .BIO Files:
 - MC0806EA_000000B4.mcb
 - MC0806EA_000000F4.pdb

Features Changes/Updates/Fixes:

1. Fixed issue where TOCTOU vulnerability in "UsbRT".
2. Updated 2023.3 Intel Platform Update.
3. Updated Harden SMM Write Flash.
4. Updated BlackLotus-Secure Boot DBX.
5. Fixed issue where Heap Buffer Overflow in TCG2MeasurePeImage.
6. Updated OpenSSL Policy Constraints.
7. Fixed issue where BIOS stack buffer overflow vulnerability.
8. Updated Update for UsbRtSmm and UsbS5Wakeup.
9. Fixed issue where After upgrading to BIOS BE0094, system no longer boots to legacy boot drive.

Known Errata:

- Windows Bitlocker Recovery will occur after reloading of the default Secure Boot key in Visual BIOS starting from BE0095. This

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

is due to an NEW updated Secure Boot DBX.

- Blocked flash / recovery downgrade to BE0092 and previous versions due to ME FW blocked downgrade.

BIOS Version 0094 - BECFL357.86A.0094.2023.0612.1527

About This Release:

- Date: June 14, 2023
- ROM Image Checksum: 0x5FAA
- EC Firmware: v3.26
- ME Firmware: 12.0.93.2331
- PMC Firmware: 300.1.20.1030
- I219 NVM: 0.4
- CRB Label: 1AUOK034
- Boot Guard ACM: 1.8.0
- Bios Guard: Based on BiosGuard_056
- Silicon initialization Code: Based on 7.0.51.41
- Memory Reference Code: 0,7,1,95
- Integrated Graphics:
 - Option ROM: v1026
 - UEFI Driver: v9.0.1098
- SATA RAID Option ROM: 17.8.0.4507
- AHCI Code: Based on AHCI_19
- LAN Option ROM: PXE V0.1.1.3
- Visual BIOS: 2.2.23
- Supported Flash Devices:

WinBond	W25Q128JVS IQ	16MB (3.3V)
Macronix	MX25L12873FM2I-10G	16MB (3.3V)
GigaDevice	GD25B127DSIGR	16MB (3.3V)
- Microcode Updates included in .ROM & .BIO Files:
 - MC0806EA_000000B4.mcb
 - MC0806EA_000000F4.pdb

Features Changes/Updates/Fixes:

- Fixed issue where EDK2 vulnerabilities.
- Fixed issue where OpenSSL vulnerabilities.
- Fixed issue where Incorrect bound check vulnerability.
- Added PlatformLang Timeout Variable Access.
- Added "SmiFlash" related solution implementation.
- Fixed issue where OOB RW vulnerability In Intel NUC.
- Fixed issue where TOCTOU vulnerability In Intel NUC.
- Updated IPU 2023.1 Update.
- Updated IPU 2023.2 Update.
- Updated ME FW to 12.0.93.2331 (v4.1).
- Updated CPU Microcode to MC0806EA_000000F4.pdb.
- Updated SATA RAID Option ROM: 17.8.0.4507

Feature Changes/Updates/Fixes:

- Blocked flash / recovery downgrade to BE0092 and previous versions due to ME FW blocked downgrade.

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

BIOS Version 0092 - BECFL357.86A.0092.2023.0214.1114**About This Release:**

- Date: February 17, 2023
- ROM Image Checksum: 0x086A
- EC Firmware: v3.26
- ME Firmware: 12.0.92.2145
- PMC Firmware: 300.1.20.1030
- I219 NVM: 0.4
- CRB Label: 1AUOK034
- Boot Guard ACM: 1.4.0
- Bios Guard: Based on BiosGuard_032
- Silicon initialization Code: Based on 7.0.51.41
- Memory Reference Code: 0,7,1,95
- Integrated Graphics:
 - Option ROM: v1026
 - UEFI Driver: v9.0.1098
- SATA RAID Option ROM: 17.8.0.1065
- AHCI Code: Based on AHCI_19
- LAN Option ROM: PXE V0.1.1.3
- Visual BIOS: 2.2.23
- Supported Flash Devices:

WinBond	W25Q128JVSIQ	16MB (3.3V)
Macronix	MX25L12873FM2I-10G	16MB (3.3V)
GigaDevice	GD25B127DSIGR	16MB (3.3V)
- Microcode Updates included in .ROM & .BIO Files:
 - MC0806EA_000000B4.mcb
 - MC0806EA_000000F0.pdb

Feature Changes/Updates/Fixes:

- Fixed issue where After upgrading to BIOS BE0090, the system no longer boots to a Legacy Boot drive.

BIOS Version 0090 - BECFL357.86A.0090.2022.0916.1942**About This Release:**

- Date: September 16, 2022
- ROM Image Checksum: 0xBCF8
- ME Firmware: 12.0.92.2145 (v3)
- EC Firmware: v3.26
- PMC Firmware: 300.1.20.1030
- I219 NVM: 0.4
- CRB Label: 1AUOK034
- Boot Guard ACM: 1.4.0
- BIOS Guard: Based on BiosGuard_032
- Silicon initialization Code: Based on 7.0.51.41
- Memory Reference Code: 0,7,1,95
- Integrated Graphics:
 - Option ROM: v1026
 - UEFI Driver: v9.0.1098

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

- SATA RAID Option ROM: 17.8.0.1065
- AHCI Code: Based on AHCI_17
- LAN Option ROM: PXE V0.1.1.3
- Visual BIOS: 2.2.23
- Supported Flash Devices:

WinBond	W25Q128JVS1Q	16MB (3.3V)
Macronix	MX25L12873FM2I-10G	16MB (3.3V)
GigaDevice	GD25B127DSIGR	16MB (3.3V)
- Microcode Updates included in .ROM & .BIO Files:

MC0806EA_000000B4.mcb
MC0806EA_000000EC.pdb

Features Change/ Update:

- Updated ME FW to 12.0.92.2145 (v3).
- Fixed issue where POST hotkey message does not display when Secure Boot is Enabled.
- Added Enable TCO timer standard token.
- Fixed issue where Unauthorized modification of UEFI variables could overwrite arbitrary SMRAM.
- Fixed issue where Unauthorized modification of UEFI variables could disable the protect mechanism of SMM.
- Fixed issue where Unauthorized modification of UEFI variables.
- Fixed issue where Privilege escalation vulnerability from kernel to SMM in multiple devices.
- Updated CPU Microcode (0xEC) for IPU 2021.2
- Updated patch will assert at all conditions, confirmed to remove from the project.
- Updated for 2021.2 IPU BIOS change.
- Fixed issue where ME minor version checking algorithm issue.
- Fixed issue where No Boot after the BIOS update via WU issue.
- Fixed issue where system can't boot up after changing settings issue.
- Fixed issue where BIOS "Enhanced Consumer IR" item incorrect value when under normal mode issue.

BIOS Version 0089 - BECFL357.86A.0089.2021.0621.1343

About This Release:

- Date: June 21, 2021
- ROM Image Checksum: 0xEDB5
- ME Firmware: 12.0.81.1753
- EC Firmware: v3.26
- Memory Reference Code: Based on 7.0.51.41
- Integrated Graphics:
 - Option ROM: v1026
 - UEFI Driver: v9.0.1098
- SATA RAID Option ROM: 17.8.0.1065
- AHCI Code: Based on AHCI_17
- LAN Option ROM: PXE V0.1.1.3
- Visual BIOS: 2.2.23

- Supported Flash Devices:

WinBond	W25Q128JVSIG	16MB (3.3V)
Macronix	MX25L12873FM2I-10G	16MB (3.3V)
GigaDevice	GD25B127DSIGR	16MB (3.3V)
- Microcode Updates included in .ROM & .BIO Files:

MC0806EA_000000B4.mcb
MC0806EA_000000EA.pdb

New Fixes/Features:

- Fixed issue with OFBD module SMI handler vulnerabilities.
- Updated CPU Microcode Firmware to 0xEA for IPU2021.1
- Fixed issue where after pressing "F10" for One Time Boot menu, pressing ESC key did not exit menu.
- Added protection code for unauthorized write at controllable address in SMRAM.
- Fixed issue to achieve arbitrary write in SMRAM save state region.

BIOS Version 0088 - BECFL357.86A.0088.2021.0330.1431

About This Release:

- Date: March 30, 2021
- ROM Image Checksum: 0x9479
- ME Firmware: 12.0.81.1753
- EC Firmware: v3.26
- Memory Reference Code: Based on 7.0.51.41
- Integrated Graphics:
 - Option ROM: v1026
 - UEFI Driver: v9.0.1098
- SATA RAID Option ROM: 17.8.0.1065
- AHCI Code: Based on AHCI_17
- LAN Option ROM: PXE V0.1.1.3
- Visual BIOS: 2.2.23
- Supported Flash Devices:

WinBond	W25Q128JVSIG	16MB (3.3V)
Macronix	MX25L12873FM2I-10G	16MB (3.3V)
GigaDevice	GD25B127DSIGR	16MB (3.3V)
- Microcode Updates included in .ROM & .BIO Files:

MC0806EA_000000B4.mcb
MC0806EA_000000E0.pdb

New Fixes/Features:

- Updated ME Firmware version to 12.0.81.1753.
- Fixed issue when changing VR Temp to CPU Temp in performance monitor.
- Updated NTFS DXE driver when parsing NTFS file system partition.
- Update BIOS code for security fixes.

Known Errata:

- Due to the Intel® ME firmware update in BIOS version 0088, you can't downgrade to version 0087 or earlier.

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

BIOS Version 0087 - BECFL357.86A.0087.2020.1209.1115

About This Release:

- Date: December 09, 2020
- ROM Image Checksum: 0x8B48
- ME Firmware: 12.0.71.1681
- EC Firmware: v3.26
- Memory Reference Code: Based on 7.0.51.41
- Integrated Graphics:
 - Option ROM: v1026
 - UEFI Driver: v9.0.1098
- SATA RAID Option ROM: 17.8.0.1065
- AHCI Code: Based on AHCI_17
- LAN Option ROM: PXE V0.1.1.3
- Visual BIOS: 2.2.23
- Supported Flash Devices:

WinBond	W25Q128JVSIQ	16MB (3.3V)
Macronix	MX25L12873FM2I-10G	16MB (3.3V)
GigaDevice	GD25B127DSIGR	16MB (3.3V)
- Microcode Updates included in .ROM & .BIO Files:

MC0806EA_000000B4.mcb
MC0806EA_000000E0.pdb

New Fixes/Features:

- Updated FITC tools.
- Updated ME Firmware to 12.0.71.1681
- Updated EC Firmware to 3.26
- Fixed issue where HDD LED kept lighting.
- Update BIOS code for security fixes.

Known Errata:

- Due to the Intel® ME firmware update in BIOS version 0087, you can't downgrade to version 0085 or earlier.

BIOS Version 0085 - BECFL357.86A.0085.2020.1007.1917

About This Release:

- Date: October 07, 2020
- ROM Image Checksum: 0x3170
- ME Firmware: 12.0.68.1606
- EC Firmware: v3.25
- Memory Reference Code: Based on 7.0.51.41
- Integrated Graphics:

Option ROM: v1026
UEFI Driver: v9.0.1098

- SATA RAID Option ROM: 17.8.0.1065
- AHCI Code: Based on AHCI_17
- LAN Option ROM: PXE V0.1.1.3
- Visual BIOS: 2.2.23
- Supported Flash Devices:

WinBond	W25Q128JVSQ	16MB (3.3V)
Macronix	MX25L12873FM2I-10G	16MB (3.3V)
GigaDevice	GD25B127DSIGR	16MB (3.3V)
- Microcode Updates included in .ROM & .BIO Files:

MC0806EA_000000B4.mcb
MC0806EA_000000D6.pdb

New Fixes/Features:

- Fixed issue that made system fans spin over 3000 RPM regardless of workload.

BIOS Version 0083 - BECFL357.86A.0083.2020.0730.1436

About This Release:

- Date: July 30, 2020
- ROM Image Checksum: 0xE4C0
- ME Firmware: 12.0.68.1606
- EC Firmware: v3.25
- Memory Reference Code: Based on 7.0.51.41
- Integrated Graphics:

Option ROM: v1026
UEFI Driver: v9.0.1098
- SATA RAID Option ROM: 17.8.0.1065
- AHCI Code: Based on AHCI_17
- LAN Option ROM: PXE V0.1.1.3
- Visual BIOS: 2.2.23
- Supported Flash Devices:

WinBond	W25Q128JVSQ	16MB (3.3V)
Macronix	MX25L12873FM2I-10G	16MB (3.3V)
GigaDevice	GD25B127DSIGR	16MB (3.3V)
- Microcode Updates included in .ROM & .BIO Files:

MC0806EA_000000B4.mcb
MC0806EA_000000D6.pdb

New Fixes/Features:

- Fixed issue where "Optane cannot work after BIOS recovery".
- Fixed issue with "Kernel DMA protection".
- Fixed issue where Thunderbolt boot was disabled after POST time improvement.
- Updated BIOS code for security fixes.
- Updated ME Firmware to 12.0.68.1606
- Update EC Firmware to v3.25.

Known Errata:

- Due to the Intel® ME firmware update in BIOS version 0083, you can't downgrade to version 0081 or earlier.

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

BIOS Version 0081 - BECFL357.86A.0081.2020.0504.1834

About This Release:

- Date: May 04, 2020
- ROM Image Checksum: 0xC513
- ME Firmware: 12.0.47.1524
- EC Firmware: v3.20
- Memory Reference Code: Based on 7.0.51.41
- Integrated Graphics:
 - Option ROM: v1026
 - UEFI Driver: v9.0.1098
- SATA RAID Option ROM: 17.8.0.1065
- AHCI Code: Based on AHCI_17
- LAN Option ROM: PXE V0.1.1.3
- Visual BIOS: 2.2.23
- Supported Flash Devices:

WinBond	W25Q128JVS IQ	16MB (3.3V)
Macronix	MX25L12873FM2I-10G	16MB (3.3V)
GigaDevice	GD25B127DSIGR	16MB (3.3V)
- Microcode Updates included in .ROM & .BIO Files:

MC0806EA_0000009D_000000B4.pdb
MC0806EA_000000CA.pdb

New Fixes/Features:

- Fixed issue with "clear security password" message.

BIOS Version 0079 - BECFL357.86A.0079.2020.0424.1838

About This Release:

- Date: April 24, 2020
- ROM Image Checksum: 0x2B0B
- ME Firmware: 12.0.47.1524
- EC Firmware: v3.20
- Memory Reference Code: Based on 7.0.51.41
- Integrated Graphics:
 - Option ROM: v1026
 - UEFI Driver: v9.0.1098
- SATA RAID Option ROM: 17.8.0.1065
- AHCI Code: Based on AHCI_17
- LAN Option ROM: PXE V0.1.1.3
- Visual BIOS: 2.2.23
- Supported Flash Devices:

WinBond	W25Q128JVS IQ	16MB (3.3V)
Macronix	MX25L12873FM2I-10G	16MB (3.3V)
GigaDevice	GD25B127DSIGR	16MB (3.3V)
- Microcode Updates included in .ROM & .BIO Files:

MC0806EA_0000009D_000000B4.pdb
MC0806EA_000000CA.pdb

New Fixes/Features:

- Fixed issue with SMM arbitrary code execution due to insufficient buffer validation.
- Fixed sleep mode issue by lock MFG mode.
- Fixed issue with USB2 port.
- Fixed issue where Crucial SSD would hang at the Intel NUC logo splash screen.
- Removed "RAM Disk Configuration" setup question.

BIOS Version 0078 - BECFL357.86A.0078.2020.0309.1538

About This Release:

- Date: March 09, 2020
- ROM Image Checksum: 0x3767
- ME Firmware: 12.0.47.1524
- EC Firmware: v3.20
- Memory Reference Code: Based on 7.0.51.41
- Integrated Graphics:
 - Option ROM: v1026
 - UEFI Driver: v9.0.1098
- SATA RAID Option ROM: 17.8.0.1065
- AHCI Code: Based on AHCI_17
- LAN Option ROM: PXE V0.1.1.3
- Visual BIOS: 2.2.23
- Supported Flash Devices:

WinBond	W25Q128JVS1Q	16MB (3.3V)
Macronix	MX25L12873FM2I-10G	16MB (3.3V)
GigaDevice	GD25B127DSIGR	16MB (3.3V)
- Microcode Updates included in .ROM & .BIO Files:

MC0806EA_0000009D_000000B4.pdb
MC0806EA_000000C6.pdb

New Fixes/Features:

- Updated the RAID Driver version to 17.8.0.1065
- Fixed issue with BIOS stress tests.
- Fixed issue where NUC logo freezes when connecting TBT monitor and HDMI monitor at the same time.
- Fixed issue regarding USB connector naming for BE products.
- Fixed issue regarding failure to PXE boot.
- Fixed issue regarding checking performance monitor and fan control mode.
- Updated BIOS code for security fixes.

BIOS Version 0077 - BECFL357.86A.0077.2019.1127.1452

About This Release:

- Date: Nov 27, 2019
- ROM Image Checksum: 0x6B9A
- ME Firmware: 12.0.47.1524
- EC Firmware: v3.20
- Memory Reference Code: Based on 7.0.51.41

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

- Integrated Graphics:
 - Option ROM: v1026
 - UEFI Driver: v9.0.1098
- SATA RAID Option ROM: 16.8.0.1000
- AHCI Code: Based on AHCI_17
- LAN Option ROM: PXE V0.1.1.3
- Visual BIOS: 2.2.23
- Supported Flash Devices:

WinBond	W25Q128JVSQ	16MB (3.3V)
Macronix	MX25L12873FM2I-10G	16MB (3.3V)
GigaDevice	GD25B127DSIGR	16MB (3.3V)
- Microcode Updates included in .ROM & .BIO Files:

MC0806EA_0000009D_000000B4.pdb
MC0806EA_000000C6.pdb

New Fixes/Features:

- Updated ME to 12.0.47.1524.
- Fixed issue where "Chassis value type changed during flash by BIO" for Microsoft request
- Fixed issue with auto detect Thunderbolt device.
- Fixed issue with basic standard speed performance.
- Fixed issue where "SMBIOS Field update BIOS" for Microsoft request.
- Fixed issue with Thunderbolt controller.
- Fixed issue finding Bluetooth device.
- Fixed issue waking up Bluetooth in Legacy mode.
- Due to ME Firmware update cannot downgrade to BIOS 0075 or previous

BIOS Version 0075 - BECFL357.86A.0075.2019.1023.1448

About This Release:

- Date: Oct 23, 2019
- ROM Image Checksum: 0xB961
- ME Firmware: 12.0.32.1421
- EC Firmware: v3.20
- Memory Reference Code: Based on 7.0.44.23
- Integrated Graphics:
 - Option ROM: v1017
 - UEFI Driver: v9.0.1084
- SATA RAID Option ROM: 16.8.0.1000
- AHCI Code: Based on AHCI_17
- LAN Option ROM: PXE V0.1.1.3
- Visual BIOS: 2.2.23
- Supported Flash Devices:

WinBond	W25Q128JVSQ	16MB (3.3V)
Macronix	MX25L12873FM2I-10G	16MB (3.3V)
GigaDevice	GD25B127DSIGR	16MB (3.3V)
- Microcode Updates included in .ROM & .BIO Files:

MC0806EA_0000009D_000000B4.pdb
MC0806EA_000000C6.pdb

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

New Fixes/Features:

- Fixed issue where changes to "Native ACPI OS PCIe Support" setting in BIOS doesn't stay.
- Implemented security fixes.
- Updated processor microcode to MC0806EA_000000C6.pdb

BIOS Version 0074 - BECFL357.86A.0074.2019.0916.1548

About This Release:

- Date: September 16, 2019
- ROM Image Checksum: 0x4B57
- ME Firmware: 12.0.32.1421
- EC Firmware: v3.20
- Memory Reference Code: Based on 7.0.44.23
- Integrated Graphics
 - Option ROM: v1017
 - UEFI Driver: v9.0.1084
- SATA RAID Option ROM: 16.8.0.1000
- AHCI Code: Based on AHCI_17
- LAN Option ROM: PXE V0.1.1.3
- Visual BIOS: 2.2.23
- Supported Flash Devices:

WinBond	W25Q128JVSIQ	16MB (3.3V)
Macronix	MX25L12873FM2I-10G	16MB (3.3V)
GigaDevice	GD25B127DSIGR	16MB (3.3V)
- Microcode Updates included in .ROM File:
MC0806EA_0000009D_000000B4.pdb
- Additional Microcode Updates included only in .BIO File:

New Fixes/Features:

- Fixed issue where Watchdog feature is triggered during stress testing.
- Updated BIOS code for BIOS recovery with USB flash drive.
- Updated Chassis type default to 0x23.
- Updated BIOS code for security fixes.

BIOS Version 0073 - BECFL357.86A.0073.2019.0618.1409

About This Release:

- Date: June 18, 2019
- ROM Image Checksum: 0xF0F3
- ME Firmware: 12.0.32.1421
- EC Firmware: v3.20
- Memory Reference Code: Based on 7.0.44.23
- Integrated Graphics:
 - o Option ROM: v1017
 - o UEFI Driver: v9.0.1084
- SATA RAID Option ROM: 16.8.0.1000
- AHCI Code: Based on AHCI_17
- LAN Option ROM: PXE V0.1.1.3
- Visual BIOS: 2.2.23
- Supported Flash Devices:

WinBond	W25Q128JVSIQ	16MB (3.3V)
Macronix	MX25L12873FM2I-10G	16MB (3.3V)

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

GigaDevice GD25B127DSIGR 16MB (3.3V)

- Microcode Updates included in .ROM & .BIO Files:
MC0806EA_0000009D_000000B4.pdb

New Fixes/Features:

- Fixed issue: Keeping monitor off when WOL from S3.
- Fixed issue: Thunderbolt Hot-plugging doesn't work when you use Legacy in the BIOS.
- Fixed issue: Blue USB 3.0 port have 5V every time when system AC power turn on/turn off.
- Updated Microcode to version MC0806EA_0000009D_000000B4.pdb.
- Remove the option "SW Control" on "RGB LED" and "Button LED" items.

BIOS Version 0071 - BECFL357.86A.0071.2019.0510.1505

About This Release:

- Date: May 10, 2019
- ME Firmware: 12.0.32.1421
- EC Firmware: v3.20
- PMC Firmware: 300.1.20.1023
- Framework Reference Code: Based on 7.0.44.23
- Memory Reference Code: Based on 7.0.44.23
- Integrated Graphics:
 - Option ROM: v1017
 - UEFI Driver: v9.0.1084
- SATA RAID Option ROM: 16.8.0.1000
- AHCI Code: Based on AHCI_17
- LAN Option ROM: PXE V0.1.1.3
- Visual BIOS: 2.2.23

New Fixes/Features:

- Fixed the issue that caused the SSD password to stop working after updating to BIOS 0064 or 0066.
- Fixed the issue where the fan settings wouldn't change when changing the "Fan Control Mode" to/from Balanced to Cool.
- Fixed the issue where wireless is disabled in the BIOS but still appears in Windows device manager.
- Changed RING LED to RGB LED in the BIOS to match the motherboard silkscreen and Technical Product Specification.
- Fixed the issue with the password prompt when BitLocker is enabled.
- Updated the BIOS code for security fixes.
- Updated Intel ME firmware to version 12.0.23.1311.
- Fixed issue when keyboard/mouse is connected to Type-C port.
- Removed option for 2048MB on IGD Aperture Size setting.
- Fixed issue where HDD password feature doesn't show in the setup menu with NVME PCIe drive.
- Updated S3 Indicator blinking behavior.
- Update Graphics Option ROM to version 1017.
- Updated Graphics UEFI driver to version 9.0.1084.
- Updated RAID Option ROM to version 16.8.0.1000.

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

BIOS Version 0051 - BECFL357.86A.0051.2018.1015.1513

About This Release:

- Date: October 15, 2018
- ME Firmware: 12.0.10.1128
- EC Firmware: v3.20
- PMC Firmware: 300.1.20.1019
- Framework Reference Code: Based on 7.0.37.50
- Integrated Graphics:
 - Option ROM: v1014
 - UEFI Driver: v9.0.1080
- LAN Option ROM: PXE v0.1.1.3
- Visual Bios: 2.2.23

New Fixes/Features:

- Fixed issue where the startup sound causes error in Device Manager.
- Updated Intel® ME firmware to version 1128.
- Updated PMC firmware to version 1019.
- Updated EC firmware to version 3.20 to fix LED behavior issue.
- Updated processor support.
- Fixed issue where remove storage password causes drive to disappear from boot manager.
- Updated watchdog event to be triggered by recovery.

BIOS Version 0048 - BECFL357.86A.0048.2018.0919.2013

About This Release:

- Date: September 19, 2018
- ME Firmware: 12.0.5.1117
- EC Firmware: v3.18
- PMC Firmware:v300.1.20.1015
- Framework Reference Code: Based on 7.0.37.50
- Integrated Graphics:
 - Option ROM: v1014
 - UEFI Driver: v9.0.1080
- LAN Option ROM: PXE v0.1.1.3
- Visual Bios: 2.2.23

New Fixes/Features:

- Updated EC Firmware to version 3.18.
- Updated BIOS item Wake from Sleep State via CIR.
- Fixed issue where power LED had abnormal behavior when system enters S4 states in modern standby mode.
- Fixed issue where system can't enter Modern Standby if NVME device is installed.

BIOS Version 0041 - BECFL357.86A.0041.2018.0719.1931

About This Release:

- Date: July 19, 2018
- ME Firmware: 12.0.5.1117
- EC Firmware: v3.14
- PMC Firmware:v300.1.20.1015

- Framework Reference Code: Based on 7.0.37.50
- Integrated Graphics:
 - Option ROM: v1014
 - UEFI Driver: v9.0.1080
- LAN Option ROM: PXE V0.1.1.3
- Visual Bios: 2.2.23

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, 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) 2018 Intel Corporation.