



BIOS Update Release Notes

PRODUCTS: NUC11PHKi7C, NUC11PHKi7CAA

BIOS Version 0065 - PHTGL579.0065.2021.1014.1705

About This Release:

- Date: Oct 14, 2021
- ROM Image Checksum: A8BF844D
- ME Firmware: 15.0.10.1574
- EC Firmware: 0C.21.00
- PMC Firmware: 150.01.20.1032
- Boot Guard ACM: 1.14.10
- Memory Reference Code: Based on 0A.00.38.51
- Integrated Graphics:
 - UEFI Driver: 17.0.1045
- Intel RST Pre-OS:
 - UEFI Driver: 18.1.1.5201
- AHCI Code: Based on AHCI_24
- Wired LAN Adapter:
 - UEFI Driver: 0.8.10
- Visual BIOS: Intel AptioV
- Supported Flash Devices:

MACRONIX	MX25L25645G	32MB
----------	-------------	------
- Microcode Updates included in .BIN & .CAP Files:
M80806C1_00000078.pdb

New Fixes/Features:

- Fixed issue to fix WD Blue SN550 causing a BSOD after waking up from MDSB.
- Updated EC Firmware to 0C.21.00
- Updated ME Firmware to 15.0.10.1574
- Fixed vulnerability issue with EFI variable read procedure.
- Implemented BIOS Guard solution for PEI buffer overflow.

Known Errata:

- If a display is connected to either Type C ports, it will not show a message when Flashing Retimer firmware.
- Due to security fixes in version 0062 you cannot downgrade to version 0056 or earlier.

BIOS Version 0063 - PHTGL579.0063.2021.0707.1057

About This Release:

- Date: Jul 7, 2021
- ROM Image Checksum: 1af8f9ea
- ME Firmware: 15.0.10.1447
- EC Firmware: 0C.19.00
- PMC Firmware: 150.01.20.1028
- Boot Guard ACM: 1.14.10

- Memory Reference Code: Based on 0A.00.38.51
- Integrated Graphics:
 - UEFI Driver: 17.0.1045
- Intel RST Pre-OS:
 - UEFI Driver: 18.1.1.5201
- AHCI Code: Based on AHCI_24
- Wired LAN Adapter:
 - UEFI Driver: 0.8.10
- Visual BIOS: Intel AptioV
- Supported Flash Devices:

MACRONIX	MX25L25645G	32MB
----------	-------------	------
- Microcode Updates included in .BIN & .CAP Files:

M80806C1_00000078.pdb

New Fixes/Features:

- Fixed issue with EC firmware spelling error when BIOS is updated.
- Changed power sequence for SD card reader.

Known Errata:

- If a display is connected to either Type C ports, it will not show a message when Flashing Retimer firmware.
- Due to security fixes in version 0062 you cannot downgrade to version 0056 or earlier.

BIOS Version 0062 - PHTGL579.0062.2021.0430.1451

About This Release:

- Date: April 30, 2021
- ROM Image Checksum: 0x63CC
- ME Firmware: 15.0.10.1447
- EC Firmware: 0C.19.00
- PMC Firmware: 150.01.20.1028
- Boot Guard ACM: 1.14.10
- Memory Reference Code: Based on 0A.00.38.51
- Integrated Graphics:
 - UEFI Driver: 17.0.1045
- Intel RST Pre-OS:
 - UEFI Driver: 18.1.1.5201
- AHCI Code: Based on AHCI_24
- Wired LAN Adapter:
 - UEFI Driver: 0.8.10
- Visual BIOS: Intel AptioV
- Supported Flash Devices:

MACRONIX	MX25L25645G	32MB
----------	-------------	------
- Microcode Updates included in .BIN & .CAP Files:

M80806C1_00000078.pdb

New Fixes/Features:

- Updated "OemModulePkg" for timeout variable support.
- Added display text message when Retimer Firmware is updated.
- Updated BIOS code for security fixes.
- Update Pre OS driver to RST_PV_18.1.1.1033 (18.1.1.5201).
- Updated CPU Microcode to M80806C1_00000078.pdb

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

- Fixed issue when using iFlashv to update BIOS.

Known Errata:

- Due to security fixes in version 0062 you cannot downgrade to version 0056 or earlier.

BIOS Version 0056 - PHTGL579.0056.2021.0105.1909

About This Release:

- Date: January 05, 2021
- ROM Image Checksum: 0xF4D0
- ME Firmware: 15.0.10.1447
- EC Firmware: 0C.17.00
- PMC Firmware: 150.01.20.1028
- Boot Guard ACM: 1.14.10
- Memory Reference Code: Based on 0A.00.34.21
- Integrated Graphics:
 - UEFI Driver: 17.0.1045
- Intel RST Pre-OS:
 - UEFI Driver: 18.0.1.1138.2
- AHCI Code: Based on AHCI_24
- Wired LAN Adapter:
 - UEFI Driver: 0.8.10
- Visual BIOS: Intel AptioV
- Supported Flash Devices:

MACRONIX	MX25L25645G	32MB
----------	-------------	------
- Microcode Updates included in .BIN & .CAP Files:

M80806C1_00000072.pdb

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) 2021 Intel Corporation.

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