



BIOS Update Release Notes

PRODUCTS: NUC11DBBi9, NUC11DBBi7, NUC11BTMi9, NUC11BTMi7

BIOS Version 0060 - DBTGL579.0060.2022.0117.1520

About This Release:

- Date: January 17, 2022
- ROM Image Checksum: 0xEFFB
- ME Firmware: 15.0.35.1898
- EC Firmware: 3.5.0
- Memory Reference Code: Based on 0A.00.4F.31
- Integrated Graphics:
 - Option ROM: NA
 - UEFI Driver: 17.0.1070
- AHCI Code: Based on AHCI_24
- LAN (i225-LM): Option ROM: 0.9.02
- Visual BIOS: Intel AptioV
- Supported Flash Devices:

WinBond	W25Q256JV	16MB
Macronix	MX77L25650F	16MB
GigaDevice	GD25B256D	16MB
- Microcode Updates included in .BIN & CAP Files:
 - MC2806D0_00000050.pdb
 - MC2806D1_0000003C.pdb

New Fixes/Features:

- Fixed issue where Power Button Menu was inaccessible to trigger after "G3".
- Fixed issue where user was not able to achieve arbitrary write in SMRAM save state region.
- Update vulnerable EFI variable read procedure.
- Fixed issue where SMM arbitrary code execution could allow attacker to modify SPI flash and launch BIOS bootkit.
- Added Windows 11 OS support.
- Fixed issue where system hanged with black screen when "F7" update BIOS/EC from DB0046/v3.3.1 to DB0050 (added GigaDevice SPI table into SPI_TYPE).
- Fixed Linux ACPI BIOS error.
- Fixed issue with BIOS QR code URL display.
- Based on DB0054 BIOS.
- Added Bluetooth PLDR support.
- Fixed abnormal shutdown during "S4".
- Implemented BIOS code to disable CNVi function
- Changed EC command port to 0x6E for runtime, reserved 0x66 for ACPI OS
- Help text missing after waking from "S5".
- Added USB porting for graphics card.
- Added Pop up warning message to user when transition bios is necessary.

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

- Updated ME Firmware to 15.0.35.1898

BIOS Version 0050 - DBTGL579.0050.2021.0802.1933

About This Release:

- Date: August 02, 2021
- ROM Image Checksum: 0x1D34
- ME Firmware: 15.0.30.1716
- EC Firmware: 3.5.0
- Memory Reference Code: Based on 0A.00.4F.31
- Integrated Graphics:
 - Option ROM: NA
 - UEFI Driver: 17.0.1061
- AHCI Code: Based on AHCI_24
- LAN (i225-LM): Option ROM: 0.9.02
- Visual BIOS: Intel AptioV
- Supported Flash Devices:

WinBond	W25Q256JV	16MB
Macronix	MX77L25650F	16MB
GigaDevice	GD25B256D	16MB
- Microcode Updates included in .BIN & .CAP Files:

MC2806D0_00000050.pdb
MC2806D1_0000002C.pdb

New Fixes/Features:

- Updated EC Firmware to v3.5.0
- Fixed issues with EC Firmware update process.
- Added VMD Port SSD Info in BIOS.
- Removed Type-C USB port control, it can be control by Thunderbolt item
- Enabled both USB ports in common IO header.
- Fixed items in iSetupCfg tool.

BIOS Version 0046 - DBTGL579.0046.2021.0705.2108

About This Release:

- Date: July 05, 2021
- ROM Image Checksum: 0x324C
- ME Firmware: 15.0.30.1716
- EC Firmware: 3.3.1
- Memory Reference Code: Based on 0A.00.4F.31
- Integrated Graphics:
 - UEFI Driver: 17.0.1061
- AHCI Code: Based on AHCI_24
- LAN (i225-LM): Option ROM: 0.9.02
- Visual BIOS: Intel AptioV
- Supported Flash Devices:
 - WinBond W25Q256JV 16MB
 - Macronix MX77L25650F 16MB
 - GigaDevice GD25B256D 16MB
- Microcode Updates included in .BIN & .CAP Files:

- MC2806D0_00000050.pdb
- MC2806D1_0000002C.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) 2022 Intel Corporation.

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