



BIOS Update Release Notes

PRODUCTS: NUC6CAYS, NUC6CAYH

BIOS Version 0070 - AYAPLCEL.86A.0070.2021.0901.1556

About This Release:

- Date: Sep 1, 2021
- ROM Image Checksum: 0xC53B
- ME Firmware: 3.1.86.2538
- EC Firmware: 22.00
- Memory Reference Code: Based on 1.2.3
- Integrated Graphics:
 - Option ROM: Build 1016 PC 14.34
 - UEFI Driver: 10.0.1036
- LAN Option ROM: PXE-2.1 (build 083)
- Visual BIOS: 2.2.23

- Supported Flash Devices:
 - WinBond W25Q128FWSIQ 16MB (1.8V)
 - MACRONIX MX25U12873F 16MB

- Microcode Updates included in .ROM & .BIO Files:
 - M03506C9_00000046.PDB

New Fixes/Features:

- Updated CPU Microcode to M03506C9_00000046.
- Fixed vulnerability with "LegacySmmSredir"_driver.

BIOS Version 0069 - AYAPLCEL.86A.0069.2021.0602.1952

About This Release:

- Date: June 03, 2021
- ROM Image Checksum: 0x184C
- TXE Firmware: 3.1.86.2538
- EC Firmware: 22.00
- Memory Reference Code: Based on 1.2.3
- Integrated Graphics:
 - Option ROM: Build 1016 PC 14.34
 - UEFI Driver: 10.0.1036
- LAN Option ROM: PXE-2.1 (build 083)
- Visual BIOS: 2.2.23

- Supported Flash Devices:
 - WinBond W25Q128FWSIQ 16MB (1.8V)
 - MACRONIX MX25U12873F 16MB

- Microcode Updates included in .ROM & .BIO Files:
 - M03506C9_00000044.PDB

New Fixes/Features:

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

- Updated TXE (ME) Firmware to 3.1.86.2538
- Fixed SMI handler vulnerabilities.
- Fixed issue where user was able to achieve arbitrary write in SMRAM save state region.
- Updated CPU Microcode to M03506C9_00000044.PDB
- Added protection code for unauthorized write at controllable address in SMRAM.

BIOS Version 0068 - AYAPLCEL.86A.0068.2021.0318.1138

About This Release:

- Date: March 18, 2021
- ROM Image Checksum: 0xA8EF
- ME Firmware: 3.1.80.2400
- EC Firmware: 22.00
- Memory Reference Code: Based on 1.2.3
- Integrated Graphics:
 - Option ROM: Build 1016 PC 14.34
 - UEFI Driver: 10.0.1036
- LAN Option ROM: PXE-2.1 (build 083)
- Visual BIOS: 2.2.23
- Supported Flash Devices:

WinBond	W25Q128FWSIQ	16MB(1.8V)
MACRONIX	MX25U12873F	16MB
- Microcode Updates included in .ROM & .BIO Files:

M03506C9_00000040.PDB

New Fixes/Features:

- Updated CPU Microcode to M03506C9_00000040
- Updated NTFS DXE driver when parsing NTFS file system partition.

BIOS Version 0067 - AYAPLCEL.86A.0067.2020.1228.1519

About This Release:

- Date: December 28, 2020
- ROM Image Checksum: 0xE3A3
- TXE Firmware: 3.1.80.2400
- EC Firmware: 22.00
- Memory Reference Code: Based on 1.2.3
- Integrated Graphics:
 - Option ROM: Build 1016 PC 14.34
 - UEFI Driver: 10.0.1036
- LAN Option ROM: PXE-2.1 (build 083)
- Visual BIOS: 2.2.23
- Supported Flash Devices:

WinBond	W25Q128FWSIQ	16MB(1.8V)
MACRONIX	MX25U12873F	16MB
- Microcode Updates included in .ROM & .BIO Files:

M03506C9_0000003C.PDB

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

New Fixes/Features:

- Updated TXE Firmware to 3.1.80.2400

BIOS Version 0066 - AYAPLCEL.86A.0066.2020.0107.1027

About This Release:

- Date: Jan 07, 2020
- ROM Image Checksum: 0x58F3
- ME Firmware: 3.1.70.2334
- EC Firmware: 22.00
- Memory Reference Code: Based on 1.2.3
- Integrated Graphics:
 - Option ROM: Build 1016 PC 14.34
 - UEFI Driver: 10.0.1036
- LAN Option ROM: PXE-2.1 (build 083)
- Visual BIOS: 2.2.23
- Supported Flash Devices:
 - WinBond W25Q128FWSIQ 16MB (1.8V)
 - MACRONIX MX25U12873F 16MB
- Microcode Updates included in .ROM & .BIO Files:
 - M03506C9_0000003C.PDB
- .ROM & .BIO Files:
 - M03506C9_0000003C.PDB

New Fixes/Features:

- Fixed issue when Intel® Dual Band Wireless-AC 8265 module disappears after reboot.
- Updated BIOS code for security fixes.

Known Errata:

- Due to the TXE firmware update in BIOS version 0066, you can't downgrade to version 0064 or earlier.

BIOS Version 0065 - AYAPLCEL.86A.0065.2019.1217.1642

About This Release:

- Date: December 17, 2019
- ROM Image Checksum: 0x9EB1
- TXE Firmware: 3.1.70.2334
- EC Firmware: 22.00
- Memory Reference Code: Based on 1.2.3
- Integrated Graphics:
 - Option ROM: Build 1016 PC 14.34
 - UEFI Driver: 10.0.1036
- LAN Option ROM: PXE-2.1 (build 083)
- Visual BIOS: 2.2.23
- Supported Flash Devices:
 - WinBond W25Q128FWSIQ 16MB(1.8V)
 - MACRONIX MX25U12873F 16MB
- Microcode Updates included in .ROM & .BIO Files:
 - M03506C9_0000003C.PDB

New Fixes/Features:

- Fixed booting issue when LAN cable is connected and DHCP is turned off on router.
- Fixed issue where "Chassis value type changed during flash by BIO" for Microsoft request.
- Updated BIOS code for security fixes.
- Added EFI ERASE BLOCK Protocol support for Android support.
- Fixed issue where "SMBIOS Field update BIOS" for Microsoft request.

BIOS Version 0064 - AYAPLCEL.86A.0064.2019.0910.1422

About This Release:

- Date: September 10, 2019
- ROM Image Checksum: 0x3E69
- ME Firmware: 3.1.60.2280
- EC Firmware: 22.00
- Memory Reference Code: Based on 1.2.3
- Integrated Graphics:
 - Option ROM: Build 1016 PC 14.34
 - UEFI Driver: 10.0.1036
- LAN Option ROM: PXE-2.1 (build 083)
- Visual BIOS: 2.2.23
- Supported Flash Devices:

WinBond	W25Q128FWSIQ	16MB (1.8V)
MACRONIX	MX25U12873F	16MB
- Microcode Updates included in .ROM & .BIO Files:
M03506C9_0000003C.PDB

New Fixes/Features:

- Updated BIOS code for security fixes.
- Updated BIOS code for BIOS recovery with USB flash drive.
- Updated Chassis type default to 0x23.
- Updated CPU microcode.

BIOS Version 0063 - AYAPLCEL.86A.0063.2019.0621.1450

About This Release:

- Date: June 21, 2019
- ME Firmware: 3.1.60.2280
- EC Firmware: 22.00
- Memory Reference Code: Based on 1.2.3
- Integrated Graphics:
 - o Option ROM: Build 1016 PC 14.34
 - o UEFI Driver: 10.0.1036
- LAN Option ROM: PXE-2.1 (build 083)
- Visual BIOS: 2.2.23

New Fixes/Features:

- Updated BIOS code for security fixes.

BIOS Version 0060 - AYAPLCEL.86A.0060.2019.0219.1527

About This Release:

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

- Date: February 19, 2019
- ME Firmware: 3.1.55.2269
- EC Firmware: 21.00
- Memory Reference Code: Based on 1.2.3
- Integrated Graphics:
 - Option ROM: Build 1016 PC 14.34
 - UEFI Driver: 10.0.1036
- LAN Option ROM: PXE-2.1 (build 083)
- Visual BIOS: 2.2.23

New Fixes/Features:

- Updated BIOS code for security fixes.

BIOS Version 0059 - AYAPLCEL.86A.0059.2018.1226.1422

About This Release:

- Date: December 26, 2018
- ME Firmware: 3.1.55.2269
- EC Firmware: 21.00
- Memory Reference Code: Based on 1.2.3
- Integrated Graphics
 - Option ROM: Build 1016 PC 14.34
 - UEFI Driver: 10.0.1036
- LAN Option ROM: PXE-2.1 (build 083)
- Visual BIOS: 2.2.23

New Fixes/Features:

- Added USB 3.0 Port Header Configuration item in BIOS Setup.

BIOS Version 0057 - AYAPLCEL.86A.0057.2018.1105.1536

About This Release:

- Date: November 5, 2018
- ME Firmware: 3.1.55.2269
- EC Firmware: 21.00
- Memory Reference Code: Based on 1.2.3
- Integrated Graphics
 - Option ROM: Build 1016 PC 14.34
 - UEFI Driver: 10.0.1036
- LAN Option ROM: PXE-2.1 (build 083)
- Visual BIOS: 2.2.23

New Fixes/Features:

- Fixed issue with PXE operations in UEFI mode.

BIOS Version 0056 - AYAPLCEL.86A.0056.2018.0926.1100

About This Release:

- Date: September 26, 2018
- ME Firmware: 3.1.55.2269
- EC Firmware: 21.00
- Memory Reference Code: Based on 1.2.3
- Integrated Graphics
 - Option ROM: Build 1016 PC 14.34

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

- o UEFI Driver: 10.0.1036
- LAN Option ROM: PXE-2.1 (build 083)
- Visual BIOS: 2.2.23

New Fixes/Features:

- BIOS functionality enhancements.

BIOS Version 0055 - AYAPLCEL.86A.0055.2018.0821.1152

About This Release:

- Date: August 21, 2018
- ME Firmware: 3.1.50.2244
- EC Firmware: 21.00
- Memory Reference Code: Based on 1.2.3
- Integrated Graphics:
 - o Option ROM: Build 1016 PC 14.34
 - o UEFI Driver: 10.0.1036
- LAN Option ROM: PXE-2.1 (build 083)
- Visual BIOS: 2.2.23

New Fixes/Features:

- Updated TXE firmware to version 3.1.55.2269.

Known Errata:

- Due to the TXE firmware update in BIOS version 0055, you can't downgrade to version 0054 or earlier.

BIOS Version 0054 - AYAPLCEL.86A.0054.2018.0809.1506

About This Release:

- Date: August 9, 2018
- ME Firmware: 3.1.50.2244
- EC Firmware: 21.00
- Memory Reference Code: Based on 1.2.3
- Integrated Graphics
 - o Option ROM: Build 1016 PC 14.34
 - o UEFI Driver: 10.0.1036
- LAN Option ROM: PXE-2.1 (build 083)
- Visual BIOS: 2.2.23

New Fixes/Features:

- Remove Ready Mode items/code in BIOS for Intel security fix.
- Set Consumer Infrared default to disabled for Windows RS4 support.

BIOS Version 0053 - AYAPLCEL.86A.0053.2018.0727.1436

About This Release:

- Date: July 27, 2018
- ME Firmware: 3.1.50.2244
- EC Firmware: 21.00
- Memory Reference Code: Based on 1.2.3
- Integrated Graphics:
 - o Option ROM: Build 1016 PC 14.34

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

- o UEFI Driver: 10.0.1036
- LAN Option ROM: PXE-2.1 (build 083)
- Visual BIOS: 2.2.23

New Fixes/Features:

- Removed Intel Ready Mode Technology setup item and set default to disabled for Intel PSIRT security fix.
- Fixed issue where while clearing the CMOS, system will boot into security jumper menu.
- Fixed issue where if remove and inject security jumper, system can't power on successfully
- Fixed issue where if press hotkey [1] in security jumper menu, it will hang on 0xFF.
- Fixed issue where if press hotkey [3] in security jumper menu, when reboot it will hang on 0xFF.

BIOS Version 0052 - AYAPLCEL.86A.0052.2018.0627.1943

About This Release:

- Date: June 27, 2018
- ME Firmware: 3.1.50.2244
- EC Firmware: 21.00
- Integrated Graphics
 - o Option ROM: Build 1016 PC 14.34
 - o UEFI Driver: 10.0.1036
- LAN Option ROM: PXE-2.1 (build 083)
- Visual BIOS: 2.2.23

New Fixes/Features:

- Updated Intel TXE to version 3.1.50.2244.
- Updated CPU Microcode (Security Advisory-00115)

BIOS Version 0051 - AYAPLCEL.86A.0051.2018.0607.1337

About This Release:

- Date: June 07, 2018
- ME Firmware: 3.1.50.2222
- EC Firmware: 21.00
- Integrated Graphics:
 - o Option ROM: Build 1016 PC 14.34
 - o UEFI Driver: 10.0.1036
- LAN Option ROM: PXE-2.1 (build 083)
- Visual BIOS: 2.2.23

New Fixes/Features:

- Updated the EC Firmware.
- Fixed CEC not working correctly.

BIOS Version 0050 - AYAPLCEL.86A.0050.2018.0521.1533

About This Release:

- Date: May 21, 2018
- ME Firmware: 3.1.50.2222
- EC Firmware: 20.00

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

- Memory Reference Code: Based on 1.2.3
- Integrated Graphics:
 - Option ROM: Build 1016 PC 14.34
 - UEFI Driver: 10.0.1036
- LAN Option ROM: PXE-2.1 (build 083)
- Visual BIOS: 2.2.23

New Fixes/Features:

- Security enhancements.
- Fixed the issue where Bluetooth would become disabled when updating the BIOS via F7.

BIOS Version 0049 - AYAPLCEL.86A.0049.2018.0508.1356

About This Release:

- Date: May 08, 2018
- ME Firmware: 3.1.50.2222
- EC Firmware: 20.00
- Memory Reference Code: Based on 1.2.3
- Integrated Graphics
 - Option ROM: Build 1016 PC 14.34
 - UEFI Driver: 10.0.1036
- LAN Option ROM: PXE-2.1 (build 083)
- Visual BIOS: 2.2.23
-

New Fixes/Features:

- Added a Bluetooth item in setup menu, and default value is enabled.
- Fixed the issue where entering the hard drive password wouldn't work.

BIOS Version 0048 - AYAPLCEL.86A.0048.2018.0420.1555

About This Release:

- Date: April 20, 2018
- ME Firmware: 3.1.50.2222
- EC Firmware: 20.00
- Memory Reference Code: Based on 1.2.3
- Integrated Graphics:
 - Option ROM: Build 1016 PC 14.34
 - UEFI Driver: 10.0.1036
- LAN Option ROM: PXE-2.1 (build 083)
- Visual BIOS: 2.2.23

New Fixes/Features:

- Security Enhancements

BIOS Version 0047 - AYAPLCEL.86A.0047.2018.0108.1419

About This Release:

- Date: January 08, 2018
- ME Firmware: 3.1.50.2222
- EC Firmware: 20.00
- Memory Reference Code: Based on 1.2.3

- Integrated Graphics
 - Option ROM: Build 1016 PC 14.34
 - UEFI Driver: 10.0.1036
- LAN Option ROM: PXE-2.1 (build 083)
- Visual BIOS: 2.2.23

New Fixes/Features:

- Updated CPU Microcode (Security Advisory-00088)
- Fixed issue where the USB 3.0 ports would run at USB 2.0 speeds.

BIOS Version 0045 - AYAPLCEL.86A.0045.2017.1218.1433

About This Release:

- Date: December 18, 2017
- ME Firmware: 3.1.50.2222
- EC Firmware: 20.00
- Memory Reference Code: Based on 1.2.3
- Integrated Graphics
 - Option ROM: Build 1016 PC 14.34
 - UEFI Driver: 10.0.1036
- LAN Option ROM: PXE-2.1 (build 083)
- Visual BIOS: 2.2.23

New Fixes/Features:

- Fixed Screen flashing issue.

BIOS Version 0043 - AYAPLCEL.86A.0043.2017.1123.1559

About This Release:

- Date: November 23, 2017
- TXE Firmware: 3.1.50.2222
- EC Firmware: 20.00
- Memory Reference Code: Based on 1.2.3
- Integrated Graphics:
 - Option ROM: Build 1016 PC 14.34
 - UEFI Driver: 10.0.1036
- LAN Option ROM: PXE-2.1 (build 083)
- Visual BIOS: 2.2.23

New Fixes/Features:

- Updated the EC version to version 20.
- Fixed the issue that when the power adapter is dis-connected and reconnected when the NUC was in S3, it would enter into "Deep S4/S5" mode.

BIOS Version 0042 - AYAPLCEL.86A.0042.2017.1117.1918

About This Release:

- Date: November 17, 2017
- TXE Firmware: 3.1.50.2222
- EC Firmware: 19.00
- PMC Firmware: 3.1a
- Framework Reference Code: Based on 1.2.3
- Integrated Graphics

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

- o Option ROM: Build 1016 PC 14.34
 - o UEFI Driver: 10.0.1036
- LAN:
 - o Option ROM: PXE-2.1 (build 083)
- Visual Bios: 2.2.23

New Fixes/Features:

- Updated Trusted Execution Engine Firmware to version: 3.1.50.2222 (Security Advisory-00086).
- Due to a security enhancement, it will not be possible to go to any BIOS earlier than BIOS 0042.
- Updated the EC version to fix an issue where the NUC couldn't be woken up with a XBOX One or XBOX 360 remote.

BIOS Version 0041 - AYAPLCEL.86A.0041.2017.0825.1152

About This Release:

- Date: August 25, 2017
- TXE Firmware: 3.0.13.1144
- EC Firmware: 18.00
- PMC Firmware: 3.1a
- Framework Reference Code: Based on 1.2.3
- Integrated Graphics
 - o Option ROM: Build 1016 PC 14.34
 - o UEFI Driver: 10.0.1036
- LAN:
 - o Option ROM: PXE-2.1 (build 083)
- Visual Bios: 2.2.23

New Fixes/Features:

- Security enhancements.
- Add setup item: "Allow UEFI 3rd party driver loaded".
- Fixed an issue where the system would not auto power on after a power failure and deep S4/S5 is enabled.

BIOS Update 0040 - AYAPLCEL.86A.0040.2017.0619.1722
--

About This Release:

- Date: June 19, 2017
- TXE Firmware: 3.0.13.1144
- EC Firmware: 18.00
- PMC Firmware: 3.1a
- Framework Reference Code: Based on 1.2.3
- Integrated Graphics
 - o Option ROM: Build 1016 PC 14.34
 - o UEFI Driver: 10.0.1036
- LAN
 - o Option ROM: PXE-2.1 (build 083)
- Visual Bios: 2.2.23

New Fixes/Features:

- Implemented BIOS recovery feature through EC initialization.

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

- Fixed the issue where the system would stop at POST code 9Ah if executing an EFI file over 300 MB.
- Fixed the issue where a USB wired mouse would move slowly after upgrading the BIOS to AY0024.
- Updated the EC version to version 18.0
- Fixed the LED effect when changing the always on mode to, low brightness slow fade mode.
- Implemented error message when trying to use the wrong BIOS.
- Fixed the issue where the LED button flashes abnormally while updating the BIOS.

BIOS Version 0038 - AYAPLCEL.86A.0038.2017.0310.1633

About This Release:

- Date: March 10, 2017
- TXE Firmware: 3.0.13.1144
- EC Firmware: 16.00
- PMC Firmware: 3.1a
- Framework Reference Code: Based on 1.2.3
- Integrated Graphics
 - Option ROM: Build 1016 PC 14.34
 - UEFI Driver: 10.0.1036
- LAN
 - Option ROM: PXE-2.1 (build 083)
- Visual Bios: 2.2.23

New Fixes/Features:

- Changed RTD3 Setup item to be disabled on default.
- Changed the EC so that it cannot be downgraded.
- Updated the EC to version 16.0.
- Updated the GOP.
- Updated new LED items.
- Added CEC help strings in BIOS setup menu.
- Enabled LPC CLKRUN number.
- Fixed issue where waking on USB from S5 would fail.
- Updated Apollo Lake smart sound technology.
- Fixed an issue where the system wouldn't boot if the startup sound was enabled or disabled via the BIOS setup menu.
- Fixed an issue where the UEFI SD card boot item is incorrect when the BIOS is set to legacy and UEFI boot.
- Updated the TXE to version 3.0.13.1144.
- Added more compatibility for ITK tool
- Fixed an issue where the NUC will not boot if shift+F10 are pressed and the Expansion card text is set to "Hide All", when the BIOS is set to legacy and UEFI boot.
- Fixed an issue where the SD card reader subsystem will display incorrectly after resuming from S3
- Fixed an issue where the rear USB 3.0 port would still detect a USB flash device when set to "Disabled".
- Fixed an issue where the Secure Jump Menu couldn't be suppressed.
- Fixed an issue where the Expansion Card Text would not show anything.
- Fixed an issue where Intel Boot Agent GE setup menu would not show anything.

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

- Updated the Apollo Lake label.
- Updated the Apollo Lake Framework BIOS Reference Code.
- Updated the CPU microcode.
- Updated the PMC firmware.
- Fixed an issue where the system always booted to the UEFI shell first.
- Fixed an issue where there would be no error message if fast boot failed on the previous boot.
- Fixed an issue where the maximum temperature setting of the fan, in custom mode, would not fill in the EC register correctly.
- Fixed an issue where, "The fixed mode default duty cycle" was incorrect.
- Fixed an issue where "Type 10: Intel High Definition Audio Device" needed to say, "Realtek High Definition Audio".

BIOS Version 0029 - AYAPLCEL.86A.0029.2016.1124.1625

About This Release:

- Date: November 24, 2016
- TXE Firmware: 3.0.11.1131
- Framework Reference Code: Based on 1.2.1
- Integrated Graphics
 - Option ROM: Build 1016 PC 14.34
 - UEFI Driver: 10.0.1035
- LAN
 - Option ROM: PXE-2.1 (build 083)
- Visual Bios: 2.2.23
- PMC FW rev : 3.19
- EC FW rev : 14.00

New Fixes/Features:

- Fixed issue where the system would always first boot to UEFI shell in BIOS 0028.
- Fixed issue where no error message would occur if the previous fast boot failed. Added maximum temperature for fan custom mod.

BIOS Version 0027 - AYAPLCEL.86A.0027.2016.1108.1529

About This Release:

- Date: November 08, 2016
- TXE Firmware: 3.0.11.1131
- Framework Reference Code: Based on 1.2.1
- Integrated Graphics
 - Option ROM: Build 1016 PC 14.34
 - UEFI Driver: 10.0.1035
- LAN
 - Option ROM: PXE-2.1 (build 083)
- Visual Bios: 2.2.23
- PMC FW rev : 3.19
- EC FW rev : 13.00

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.