



## BIOS Update Release Notes

### PRODUCTS:NUC13ANxi3/5/7, NUC13VYxi5/7

BIOS Version 0029 - ANRPL357.0029.2023.1109.1805

#### About This Release:

- Date: Nov 09, 2023
- ROM Image Checksum: 0x9684042D
- EC Firmware: 0A.15.00
- ME Firmware: 16.1.30.2264
- PCH Configuration Firmware: 16.1.0.1014
- PMC Firmware: 160.1.0.1029
- iTBT Firmware: TBT\_ADLRPL\_MUPHPX\_All\_19.1V1\_Rel\_ALL\_Prod\_PV1
- IOM Firmware: 24.0006.0.0
- Retimer Firmware in BIOS capsule:
  - INTEL\_NUC13AN\_0x3037\_ARENA\_CANYON\_NONVPRO\_BBR\_CDR\_A1\_ADL\_P\_LP4\_PORTS\_0\_1\_rev3\_10\_TI\_SEC3\_sign.bin
  - INTEL\_NUC13AN\_0x3038\_ARENA\_CANYON\_VPRO\_BBR\_CDR\_A1\_ADL\_P\_LP4\_PORTS\_0\_1\_rev3\_10\_TI\_SEC3\_sign.bin
- NPHY Firmware: RPLP\_NPHY\_REL\_PV\_14.530.508.8257
- i226 NVM:
  - FXVL\_125C\_V\_1MB\_2.17.bin
  - FXVL\_125B\_LM\_1MB\_2.17.bin
- CRB Label: 5.27\_1AYRT\_RC0C.00.93.20(3503.00)\_033
- Boot Guard ACM: v 1.18.16
- BIOS Guard: BiosGuard\_039
- Silicon Initialization Code: 0C.00.93.20
- Memory Reference Code: 0.0.4.116
- Integrated Graphics:
  - UEFI Driver: 21.0.1061
- Intel RST Pre-OS:
  - VMD UEFI Driver: 19.5.5.5727
- AHCI Code: AHCI\_31
- Visual BIOS: Intel AptioV
- Supported Flash Devices:
  - WinBond W25R256JVEIQ 32MB
  - Macronix MX77L25650FZ4I42 32MB
  - GigaDevice GD25R256EYIGR 32MB
- Microcode Updates included in .BIN & .CAP Files:
  - MC0B06A2\_0000411C.pdb

#### Feature Changes/Updates/Fixes:

- Updated IPU2023.3 Intel Platform Update.
- Fixed issue where LogoFAIL vulnerability.
- Fixed issue where S3 Sleep/Wake-Up cycle.
- Fixed issue where TOCTOU vulnerability in "SmiFlash".
- Fixed issue where Intel NUC information leak vulnerability.
- Updated Harden SMM Write Flash area.

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

- Updated L10 Sku list.
- Updated ME FW to 16.1.30.2264.
- Updated CPU Microcode to MC0B06A2\_0000411C.pdb.
- Fixed issue where Can't exit BIOS Setup when pressing the Exit button.

<b>BIOS Version 0027 - ANRPL357.0027.2023.0607.1754</b>
---

#### **About This Release:**

- Date: June 07, 2023
- ROM Image Checksum: 0x961DC36B
- EC Firmware: 0A.15.00
- ME Firmware: 16.1.25.2091
- PCH Configuration Firmware: 16.1.0.1014
- PMC Firmware: 160.1.0.1029
- iTBT Firmware: TBT\_ADLRPL\_MUPHPX\_All\_19.1V1\_Rel\_ALL\_Prod\_PV1
- IOM Firmware: 24.0006.0.0
- Retimer Firmware in BIOS capsule:
  - INTEL\_NUC13AN\_0x3037\_ARENA\_CANYON\_NONVPRO\_BBR\_CDR\_A1\_ADL\_P\_LP4\_PORTS\_0\_1\_rev3\_10\_TI\_SEC3\_sign.bin
  - INTEL\_NUC13AN\_0x3038\_ARENA\_CANYON\_VPRO\_BBR\_CDR\_A1\_ADL\_P\_LP4\_PORTS\_0\_1\_rev3\_10\_TI\_SEC3\_sign.bin
- NPHY Firmware: RPLP\_NPHY\_REL\_PV\_14.530.508.8257
- I226 NVM:
  - FXVL\_125C\_V\_1MB\_2.17.bin
  - FXVL\_125B\_LM\_1MB\_2.17.bin
- CRB Label: 5.27\_1AYRT\_RC0C.00.93.20(3503.00)\_033
- Boot Guard ACM: v 1.18.13
- BIOS Guard: BiosGuard\_039
- Silicon Initialization Code: 0C.00.93.20
- Memory Reference Code: 0.0.4.116
- Integrated Graphics:
  - UEFI Driver: 21.0.1061
- Intel RST Pre-OS:
  - VMD UEFI Driver: 19.5.0.5676
- AHCI Code: AHCI\_31
- Visual BIOS: Intel AptioV
- Supported Flash Devices:
 

◦ WinBond	W25R256JVEIQ	32MB
◦ Macronix	MX77L25650FZ4I42	32MB
◦ GigaDevice	GD25R256EYIGR	32MB
- Microcode Updates included in .BIN & .CAP Files:
  - MC0B06A2\_0000410E.pdb

#### **Feature Changes/Updates/Fixes:**

- Fixed issue where UEFI Variable access vulnerability.
- Fixed issue where "SmmEntryPoint" Underflow vulnerability.
- Added Implement Intel Ethernet Controller i225/i226 Windows Capsule Update SDK.
- Added Add new function: Software Control for Display Emulation.
- Added Add back IGD Primary Video Port and IGD Secondary Video

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

Port items.

- Updated WMI method which needs to access EC needs to go for BIOS ASL implementation.
- Updated EC FW to 0A.15.00.
- Updated Power setting "PL4" to 102w for Core i5/i7 sku.
- Updated Update Fan table according to AN\_VY fan table and PL setting revised\_20230526\_pegaxlsx.xlsx.
- Added Wi-Fi 6E support for Japan.
- Fixed issue where System can't find the TPM after "BIOS Load Optimized Defaults" with disabled "Intel Platform Trust Technology (Non-vPro)" or "Trusted Platform Module 2.0 Presence (vPro)" status.
- Fixed issue where After setting all USB ports to "No Detect", User could not use a USB keyboard when in the "Power Button Menu".
- Fixed issue where Abnormal screen after executing "Perform Platform Erase" operations to erase an SSD device.
- Fixed issue where Missing the EC FW version on SMBIOS page.
- Fixed issue where Reserve Offset "0x481h" bit7.

<b>BIOS Version 0026 - ANRPL357.0026.2023.0314.1458</b>
---

**About This Release:**

- Date: 03/14/2023
- ROM Image Checksum: 0x966C86EC
- EC Firmware: 0A.14.00
- ME Firmware: 16.1.25.2091
- PCH Configuration Firmware: 16.1.0.1014
- PMC Firmware: 160.1.0.1029
- iTBT Firmware: TBT\_ADLRPL\_MUPHPX\_All\_19.1V1\_Rel\_ALL\_Prod\_PV1
- IOM Firmware: 24.0006.0.0
- Retimer Firmware in BIOS capsule:
  - INTEL\_NUC13AN\_0x3037\_ARENA\_CANYON\_NONVPRO\_BBR\_CDR\_A1\_ADL\_P\_LP4\_PORTS\_0\_1\_rev3\_10\_TI\_SEC3\_sign.bin
  - INTEL\_NUC13AN\_0x3038\_ARENA\_CANYON\_VPRO\_BBR\_CDR\_A1\_ADL\_P\_LP4\_PORTS\_0\_1\_rev3\_10\_TI\_SEC3\_sign.bin
- NPHY Firmware: RPLP\_NPHY\_REL\_PV\_14.530.508.8257
- I226 NVM:
  - FXVL\_125C\_V\_1MB\_2.17.bin
  - FXVL\_125B\_LM\_1MB\_2.17.bin
- CRB Label: 5.27\_1AYRT\_RC0C.00.93.20(3503.00)\_033
- Boot Guard ACM: v 1.18.13
- Bios Guard: BiosGuard\_039
- Silicon Initialization Code: 0C.00.93.20
- Memory Reference Code: 0.0.4.116
- Integrated Graphics:
  - UEFI Driver: 21.0.1061
- Intel RST Pre-OS:
  - VMD UEFI Driver: 19.5.0.5676
- AHCI Code: AHCI\_31
- Visual BIOS: Intel AptioV
- Supported Flash Devices:
  - Winbond W25R256JVEIQ 32MB

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

- o Macronix MX77L25650FZ4I42 32MB
  - o GigaDevice GD25R256EYIGR 32MB
- Microcode Updates included in .BIN & .CAP Files:
  - o MC0B06A2\_0000410E.pdb

#### **Feature Change/Update:**

- Added Implement NUC13VY SKU number into BIOS for ES logo.
- Updated Set IGD Secondary Video Port to "None" if IGD Primary Video Port is "Auto". (this item is hidden in AN0025).
- Fixed issue where PXE and HTTP boot options issue.

### **BIOS Version 0025 - ANRPL357.0025.2023.0222.0859**

#### **About This Release:**

- Date: 02/22/2023
- ROM Image Checksum: 0x966E9E2F
- EC Firmware: 0A.14.00
- ME Firmware: 16.1.25.2091
- PCH Configuration Firmware: 16.1.0.1014
- PMC Firmware: 160.1.0.1029
- iTBT Firmware: TBT\_ADLRPL\_MUPHPX\_All\_19.1V1\_Rel\_ALL\_Prod\_PV1
- IOM Firmware: 24.0006.0.0
- Retimer Firmware in BIOS capsule:
  - o INTEL\_NUC13AN\_0x3037\_ARENA\_CANYON\_NONVPRO\_BBR\_CDR\_A1\_ADL\_P\_LP4\_PORTS\_0\_1\_rev3\_10\_TI\_SEC3\_sign.bin
  - o INTEL\_NUC13AN\_0x3038\_ARENA\_CANYON\_VPRO\_BBR\_CDR\_A1\_ADL\_P\_LP4\_PORTS\_0\_1\_rev3\_10\_TI\_SEC3\_sign.bin
- NPHY Firmware: RPLP\_NPHY\_REL\_PV\_14.530.508.8257
- I226 NVM:
  - o FXVL\_125C\_V\_1MB\_2.17.bin
  - o FXVL\_125B\_LM\_1MB\_2.17.bin
- CRB Label: 5.27\_1AYRT\_RC0C.00.93.20(3503.00)\_033
- Boot Guard ACM: v 1.18.13
- Bios Guard: BiosGuard\_039
- Silicon Initialization Code: 0C.00.93.20
- Memory Reference Code: 0.0.4.116
- Integrated Graphics:
  - o UEFI Driver: 21.0.1061
- Intel RST Pre-OS:
  - o VMD UEFI Driver: 19.5.0.5676
- AHCI Code: AHCI\_31
- Visual BIOS: Intel AptioV
- Supported Flash Devices:
  - o WinBond W25R256JVEIQ 32MB
  - o Macronix MX77L25650FZ4I42 32MB
  - o GigaDevice GD25R256EYIGR 32MB
- Microcode Updates included in .BIN & .CAP Files:
  - o MC0B06A2\_0000410E.pdb

#### **New Fixes/Features:**

- Initial production BIOS release

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

---

---

## 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.