



BIOS Update Release Notes

PRODUCTS: LAPRC510, LAPRC710

BIOS Version 0070 - RCADL357.0070.2025.0618.1619

About This Release:

- Date: 06/18/2025
- ROM Image Checksum: 0x99A3FFFA
- ME Firmware: 16.1.38.2676
- EC Firmware: 00.22.00.000
- PCH Configuration Firmware: 16.0.0.1014
- PMC Firmware: 160.1.0.1030
- iTBT Firmware: 16.1.35.2212
- IOM Firmware: 36.7.0.0000
- Retimer Firmware in BIOS capsule: NA
- SPHY Firmware: NA
- NPHY Firmware: 14.531.509.8259
- Platform Properties Assessment Module: 11.23r.4
- I219 NVM: NA
- CRB Label: 1AXFE052
- Boot Guard ACM: 1.18.15
- Bios Guard: 2.0.5021
- Silicon Initialization Code: 0C.00.69.74
- Memory Reference Code: Based on 0.0.4.6
- Intel RST Pre-OS: NA
- VMD UEFI Driver: NA
- AHCI Code: AHCI_30
- MEBx Revision: NA
- Integrated Graphics
 - UEFI Driver: 21.0.1054
- SATA RAID Option ROM: NA
- SATA non-RAID Option ROM: NA
- AHCI Code: Based on NA
- LAN Option ROM: NA
- Visual BIOS: NA
- Supported Flash Devices:
 - WinBond W25Q256FV 32MB
 - GigaDevice GD25B256D 32MB
- Microcode Updates included in .ROM File:
 - M80906A3_00000437.pdb

Feature Change/Update:

- Updated Update ME to 16.1.38.2676
- Updated 2025.2 Intel Platform Update
- Fixed issue where Implement S3 reboot code in MS support project

BIOS Version 0069 - RCADL357.0069.2025.0219.1341

About This Release:

- Date: Feb 19, 2025
- ROM Image Checksum: 0x99AB9C64
- ME Firmware: 16.1.35.2557
- EC Firmware: 00.22.00.000
- PCH Configuration Firmware: 16.0.0.1014
- PMC Firmware: 160.1.0.1030
- iTBT Firmware: 16.0.0.2102
- IOM Firmware: 36.7.0.0000
- NPHY Firmware: 14.531.509.8259
- Platform Properties Assessment Module: 11.23r.4
- CRB Label: 1AXFE052
- Boot Guard ACM: 1.18.15
- Bios Guard: 2.0.5021
- Silicon Initialization Code: 0C.00.69.74
- Memory Reference Code: Based on 0.0.4.6
- AHCI Code: AHCI_30
- Integrated Graphics:
 - UEFI Driver: 21.0.1054
- Visual BIOS: Intel AptioV
- Supported Flash Devices:

WinBond	W25Q256FV	32MB
GigaDevice	GD25B256D	32MB
- Microcode Updates included in .BIN & .CAP Files:
M80906A3_00000436.pdb

Feature Changes/Updates/Fixes:

- Fixed issue where SUT could not boot into OS on NVMe ports in config mode of Security Jumper
- Updated 2025.1 Intel Platform Update (Update)
- Fixed issue where Run "BCDEDIT /set {fwbootmgr}" timeout fail under OS

BIOS Version 0068 - RCADL357.0068.2024.1127.1548

About This Release:

- Date: Nov 27, 2024
- ROM Image Checksum: 0x99AAACAA
- ME Firmware: 16.1.35.2557
- EC Firmware: 00.22.00.000
- PCH Configuration Firmware: 16.0.0.1014
- PMC Firmware: 160.1.0.1030
- iTBT Firmware: 16.0.0.2102
- IOM Firmware: 36.7.0.0000
- NPHY Firmware: 14.531.509.8259
- Platform Properties Assessment Module: 11.23r.4
- CRB Label: 1AXFE052
- Boot Guard ACM: 1.18.15
- Bios Guard: 2.0.5021
- Silicon Initialization Code: 0C.00.69.74

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

- Memory Reference Code: Based on 0.0.4.6
- AHCI Code: AHCI_30
- Integrated Graphics:
 - UEFI Driver: 21.0.1054
- Visual BIOS: Intel AptioV
- Supported Flash Devices:

WinBond	W25Q256FV	32MB
GigaDevice	GD25B256D	32MB
- Microcode Updates included in .BIN & .CAP Files:

M80906A3_00000436.pdb

Feature Changes/Updates/Fixes:

- Updated 2024.3 Intel Platform Update
- Updated 2024.2 Intel Platform Update
- Updated 2024.4 Intel Platform Update
- Updated 2025.1 Intel Platform Update
- Updated Update CPU Microcode to 0x436
- Updated Update ME to 16.1.35.2557
- Fixed issue where Security Jumper (Config Mode) - SUT could not boot into OS on NVMe ports
- Fixed issue where Setting the Hard Disk pre-delay will cause a black screen for a period of time during the POST process.

BIOS Version 0067 - RCADL357.0067.2024.0821.1631

About This Release:

- Date: Aug 21, 2024
- ROM Image Checksum: 0x99EE52FD
- ME Firmware: 16.1.32.2418
- EC Firmware: 00.22.00.000
- PCH Configuration Firmware: 16.0.0.1014
- PMC Firmware: 160.1.0.1030
- iTBT Firmware: 16.0.0.2102
- IOM Firmware: 36.7.0.0000
- NPHY Firmware: 14.531.509.8259
- Platform Properties Assessment Module: 11.23r.4
- CRB Label: 1AXFE052
- Boot Guard ACM: 1.18.15
- Bios Guard: 2.0.5021
- Silicon Initialization Code: 0C.00.69.74
- Memory Reference Code: Based on 0.0.4.6
- AHCI Code: AHCI_30
- Integrated Graphics:
 - UEFI Driver: 21.0.1054
- Visual BIOS: Intel AptioV
- Supported Flash Devices:

WinBond	W25Q256FV	32MB
GigaDevice	GD25B256D	32MB

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

- Microcode Updates included in .BIN & .CAP Files:
M80906A3_00000435.pdb

Feature Changes/Updates/Fixes:

- Updated Update CPU Microcode to 0x435
- Updated Update ME to 16.1.32.2418
- Fixed issue where After re-plugging TYPE-C/DP/HDMI, the secure boot violation message screen shows noise
- Fixed issue where EBU will fail if rerunning the EBU program after closed it

BIOS Version 0066 - RCADL357.0066.2024.0515.1039

About This Release:

- Date: May 15, 2024
- ROM Image Checksum: 0x99F753AC
- ME Firmware: 16.1.30.2307
- EC Firmware: 00.22.00.000
- PCH Configuration Firmware: 16.0.0.1014
- PMC Firmware: 160.1.0.1030
- iTBT Firmware: 16.0.0.0202
- IOM Firmware: 36.6.0.0000
- NPHY Firmware: 14.531.509.8259
- Platform Properties Assessment Module: 11.23r.4
- CRB Label: 1AXFE052
- Boot Guard ACM: 1.18.15
- Bios Guard: 2.0.5021
- Silicon Initialization Code: 0C.00.69.74
- Memory Reference Code: Based on 0.0.4.6
- AHCI Code: AHCI_30
- Integrated Graphics:
 - UEFI Driver: 21.0.1054
- Visual BIOS: Intel AptioV
- Supported Flash Devices:

WinBond	W25Q256FV	32MB
GigaDevice	GD25B256D	32MB
- Microcode Updates included in .BIN & .CAP Files:
M80906A3_00000433.pdb

Feature Changes/Updates/Fixes:

- Fixed issue where Extended Image Parser Corruption Correction
- Fixed issue where Vulnerabilities in EDK2 NetworkPkg
- Fixed issue where TOCTOU Vulnerability in SmiFlash (Enhancement)
- Updated Update MCU to 0x433
- Fixed issue where The POST screen is not correct after the BIOS block downgrade message is displayed.
- Updated Align MRC to IPU 2024.1 from RPL CRB048

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

BIOS Version 0065 - RCADL357.0065.2024.0220.1439

About This Release:

- Date: Feb 20, 2024
- ROM Image Checksum: 0x9A06912D
- ME Firmware: 16.1.30.2307
- EC Firmware: 00.22.00.000
- PCH Configuration Firmware: 16.0.0.1014
- PMC Firmware: 160.1.0.1030
- iTBt Firmware: 16.0.0.0202
- IOM Firmware: 36.6.0.0000
- NPHY Firmware: 14.531.509.8259
- Platform Properties Assessment Module: 11.23r.4
- CRB Label: 1AXFE052
- Boot Guard ACM: 1.18.15
- Bios Guard: 2.0.5021
- Silicon Initialization Code: 0C.00.69.74
- Memory Reference Code: Based on 0.0.4.6
- AHCI Code: AHCI_30
- Integrated Graphics:
 - UEFI Driver: 21.0.1054
- Visual BIOS: Intel AptioV
- Supported Flash Devices:

WinBond	W25Q256FV	32MB
GigaDevice	GD25B256D	32MB
- Microcode Updates included in .BIN & .CAP Files:
M80906A3_00000432.pdb

Feature Changes/Updates/Fixes:

- Fixed issue where Flash driver security review
- Fixed issue where UsbRt TOCTOU Vulnerability
- Fixed issue where Image Parser Corruption Vulnerability
- Fixed issue where UsbRtSmm Vulnerability
- Fixed issue where LogoFAIL Vulnerability (patch update)
- Updated 2024.1 Intel Platform Update
- Updated 2023.4 Intel Platform Update
- Updated Update ME to 16.1.30.2307
- Updated Update CPU Microcode to M80906A3_00000432.pdb
- Updated Update Intel KEK/DB keys to support MSFT CA 2023

BIOS Version 0064 - RCADL357.0064.2023.1114.1753

About This Release:

- Date: Nov 14, 2023
- ROM Image Checksum: 0x96C83DEE
- ME Firmware: 16.1.27.2176
- EC Firmware: 00.22.00.000
- PCH Configuration Firmware: 16.0.0.1012
- PMC Firmware: 160.1.0.1029

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

- iTBT Firmware: 16.0.0.1901
- IOM Firmware: 36.6.0.0000
- NPHY Firmware: 14.530.508.8257
- Platform Properties Assessment Module: 11.23r.4
- CRB Label: 1AXFE052
- Boot Guard ACM: 1.18.15
- Bios Guard: 2.0.5021
- Silicon Initialization Code: 0C.00.69.74
- Memory Reference Code: Based on 0.0.4.6
- AHCI Code: AHCI_30
- Integrated Graphics:
 - UEFI Driver: 21.0.1054
- Visual BIOS: Intel AptioV
- Supported Flash Devices:

WinBond	W25Q256FV	32MB
GigaDevice	GD25B256D	32MB
- Microcode Updates included in .BIN & .CAP Files:

M80906A3_00000430.pdb

Feature Changes/Updates/Fixes:

- Fixed issue where LogoFAIL vulnerability.
- Fixed issue where EDK2 PEI-Phase Denial of Service vulnerability.
- Fixed issue where TOCTOU vulnerability in "SmiFlash".
- Updated CPU Microcode to M80906A3_00000430.pdb.
- Fixed issue where The values of iSetupCfg password check setting cannot be saved when pressing the Save icon in the upper right corner.

BIOS Version 0063 - RCADL357.0063.2023.0821.1414

About This Release:

- Date: Aug 21, 2023
- ROM Image Checksum: 0x96D21238
- ME Firmware: 16.1.27.2176
- EC Firmware: 00.22.00.000
- PCH Configuration Firmware: 16.0.0.1012
- PMC Firmware: 160.1.0.1029
- iTBT Firmware: 16.0.0.1901
- IOM Firmware: 36.6.0.0000
- NPHY Firmware: 14.530.508.8257
- Platform Properties Assessment Module: 11.23r.4
- CRB Label: 1AXFE052
- Boot Guard ACM: 1.18.15
- BIOS Guard: 2.0.5021
- Silicon Initialization Code: 0C.00.69.74
- Memory Reference Code: Based on 0.0.4.6
- AHCI Code: AHCI_30
- Integrated Graphics:
 - UEFI Driver: 21.0.1054
- Visual BIOS: Intel AptioV

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

- Supported Flash Devices:

WinBond	W25Q256FV	32MB
GigaDevice	GD25B256D	32MB
- Microcode Updates included in .BIN & .CAP Files:
M80906A3_0000042C.pdb

Feature Changes/Updates/Fixes:

- Updated SecureBoot DBX Update.
- Updated Harden SMM Write Flash support.
- Fixed issue where OpenSSL vulnerabilities.
- Fixed issue where Heap Buffer Overflow in TCG2MeasurPeImage.
- Updated IPU 2023.3 Update.
- Updated Support for latest flash tool: iFlashV 5.13.00.2106 (X64) / 5.13.00.2106 (IA32).

BIOS VERSION 0062 - RCADL357.0062.2023.0607.1517

About This Release:

- Date: June 07, 2023
- ROM Image Checksum: 0x9761A107
- ME Firmware: 16.1.27.2176
- EC Firmware: 00.22.00.000
- PCH Configuration Firmware: 16.0.0.1012
- PMC Firmware: 160.1.0.1029
- iTBT Firmware: 16.0.0.1901
- IOM Firmware: 36.6.0.0000
- NPHY Firmware: 14.530.508.8257
- CRB Label: 1AXFE052
- Boot Guard ACM: 1.18.10
- Bios Guard: 2.0.5021
- Silicon Initialization Code: 0C.00.69.74
- Memory Reference Code: Based on 0.0.4.6
- AHCI Code: AHCI_30
- Integrated Graphics:
 - UEFI Driver: 21.0.1054
- Visual BIOS: Intel AptioV
- Supported Flash Devices:

WinBond	W25Q256FV	32MB
GigaDevice	GD25B256D	32MB
- Microcode Updates included in .BIN & .CAP Files:
M80906A3_0000042C.pdb

Feature Changes/Updates/Fixes:

- Fixed the GenericSio Information Disclosure vulnerability.
- Added the PlatformLang Timeout Variable Access.
- Fixed the EDK2 vulnerabilities.
- Updated IPU to 2023.1.
- Fixed the OpenSSL vulnerabilities.

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

- Fixed the "SmmEntryPoint" Underflow vulnerability.
- Fixed the Intel NUC information leak vulnerability.
- Fixed the UEFI Variable access vulnerability.
- Added the "Extend CSME Measurement to TPM-PCR" function.
- Updated ME FW to version 16.1.27.2176 (v2).
- Updated the CPU Microcode to 0x42C.
- Fixed the issue where the BIOS update through the Power Button Menu [F7] Flash option fails when the Thunderbolt support items are disabled in the BIOS.

BIOS Version 0061 - RCADL357.0061.2023.0218.1043

About This Release:

- Date: 02/18/2023
- ROM Image Checksum: 0x97CB926B
- ME Firmware: 16.1.25.1865
- EC Firmware: 00.22.00.000
- PCH Configuration Firmware: 16.0.0.1012
- PMC Firmware: 160.1.0.1028
- iTBT Firmware: 16.0.0.1705
- IOM Firmware: 36.4.0.0000
- NPHY Firmware: 14.528.505.8211
- CRB Label: 1AXFE052
- Boot Guard ACM: 1.18.10
- Bios Guard: 2.0.5021
- Silicon Initialization Code: 0C.00.69.74
- Memory Reference Code: Based on 0.0.4.6
- AHCI Code: AHCI_30
- Integrated Graphics:
 - UEFI Driver: 21.0.1054
- Visual BIOS: Intel AptioV
- Supported Flash Devices:

WinBond	W25Q256FV	32MB
GigaDevice	GD25B256D	32MB
- Microcode Updates included in .BIN & .CAP Files:

M80906A3_00000429.pdb

Feature Changes/Updates/Fixes:

- Fixed issue where SDIO_DEV_CONFIGURATION SetVariable NVRAM Corruption.
- Fixed issue where UEFI Boot Variables Access.
- Fixed issue where "OpenSSL" (CVE-2022-3786 & CVE-2022-3602) security vulnerabilities.
- Fixed issue where GRUB Bootloader Vulnerability.
- Fixed issue where Intel NUC information disclosure vulnerability.
- Fixed issue where TianoCore Security Issues.

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

- Fixed issue where The stack buffer overflow vulnerability leads to arbitrary code execution in DXE driver on select Intel platforms.
- Added Adding BIOS Setup item for BIOS WU function support.
- Fixed issue where With Admin Password set, and User Access Level configured, POST Hotkeys, POST hotkey F8 should not pop-up the password prompt.
- Fixed issue where Duplicated UQI value issue fix.
- Fixed issue where iSetupCfg tool displays the unexpected message, "WARNING: Duplicate questions".
- Fixed issue where TBT GR card power-on hang code. BIOS POST hang w/TBT GR card connected.
- Fixed issue where BIOS Setup menu will hang while cursor quick click on scrollbar.
- Fixed issue where BIOS WU:DF - InfVerif INF Verification-Fails.
- Fixed issue where System cannot boot to OS after suppressing BIOS Jumper Recovery Menu until the BIOS Security Jumper was replaced.

BIOS Version 0060 - RCADL357.0060.2022.1021.1526

About This Release:

- Date: Oct 21, 2022
- ROM Image Checksum: 35A1
- ME Firmware: 16.1.25.1865
- EC Firmware: 00.22.00.000
- PCH Configuration Firmware: 16.0.0.1012
- PMC Firmware: 160.1.0.1028
- iTBT Firmware: 16.0.0.1705
- IOM Firmware: 36.4.0.0000
- NPHY Firmware: 14.528.505.8211
- CRB Label: 1AXFE052
- Bios Guard: 2.0.5021
- Memory Reference Code: Based on 0.0.4.6
- AHCI Code: AHCI_30
- Integrated Graphics:
 - UEFI Driver: 21.0.1054
- Visual BIOS: Intel AptioV
- Supported Flash Devices:

WinBond	W25Q256FV	32MB
GigaDevice	GD25B256D	32MB
- Microcode Updates included in .BIN & .CAP Files:

M80906A3_00000423.pdb

New Fixes/Features:

- Updated E-labeling to v1.1.
- Updated CPU Microcode to 0x423.
- Updated CRB to 5.26_1AXFE_RC0C.00.69.74(3253.00)_052
- Updated ME FW to 16.1.25.1865
- Updated EC FW to PL5AUXC_EC00.22.00.00 (00.22.00.00)

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

- Updated 2022 IPU update: 2022.3.
- Fixed issue where Potential hack of EBU DLL.
- Updated PTK2712, SA50151 patch.
- Fixed issue where SMM memory corruption vulnerability in SMM driver on Intel platforms.
- Fixed issue where vulnerability/info leak vulnerability.
- Fixed issue where System cannot bring USB back to work in BIOS after disabling all the USB ports in the BIOS Setup USB menu.
- Updated Follow RC0C.00.71.76(3275.00) to revert TME TPM log change.
- Fixed issue where Modify display wording in Config Mode.
- Added Variable Struct Counter.
- Added StdDefaults into ProtectedNvVariableForRuntime ELink.
- Fixed issue where iSetupCfg not able to change default value of PLx/Fan cuver parameters due to stdDefault override mechanism.

BIOS Version 0056 - RCADL357.0056.2022.0706.1057

About This Release:

- Date: July 06 2022
- ROM Image Checksum: 0x9CA02751
- ME Firmware: 16.0.15.1735
- EC Firmware: 0.21.00.00
- PMC Firmware: 160.01.00.1023
- Boot Guard ACM: 1.18.09
- Reference Code: Based on 0C.00.65.70
- Memory Reference Code: Based on 0.0.3.128
- Integrated Graphics:
 - UEFI Driver: 21.0.1046
- Visual BIOS: Intel AptioV
- Supported Flash Devices:
 - WinBond W25Q256FV 32MB
 - GigaDevice GD25B256D 32MB
- Microcode Updates included in .BIN & .CAP Files:
 - M80906A3_0000041E.pdb

New Fixes/Features:

1. Updated CPU Microcode to M80906A3_0000041E
2. Added Enabled SETUP_EXIT_MFG_SUPPORT.
3. Fixed issue where Vulnerability PTK2699.
4. Fixed issue where Vulnerability in PEI module PTK2702.
5. Changed Disable FIVR by default.
6. Changed Disabled "PchUsb2SusWellPgEnable".
7. Fixed issue Add panel flicker work-around for platforms using internal 1.05v VR.
8. Updated EC FW updated to 00.21.00.00

BIOS Version 0053 - RCADL357.0053.2022.0512.2055

About This Release:

- Date: May 12, 2022

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

- ROM Image Checksum: 0x9CBEF8BB
- ME Firmware: 16.0.15.1735
- EC Firmware: 0.20.00.00
- PMC Firmware: 160.01.00.1023
- Boot Guard ACM: 1.18.09
- Reference Code: Based on 0C.00.65.70
- Memory Reference Code: Based on 0.0.3.128
- Integrated Graphics:
 - UEFI Driver: 21.0.1046
- Visual BIOS: Intel AptioV

- Supported Flash Devices:
 - WinBond W25Q256FV 32MB
 - GigaDevice GD25B256D 32MB

- Microcode Updates included in .BIN & .CAP Files:
 - M80906A3_0000041b.pdb

New Fixes/Features:

- Initial BIOS version.

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.