



BIOS Update Release Notes

PRODUCTS: LAPRC510, LAPRC710

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.
- 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.

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

- 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)
- 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.

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

- 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
- 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

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

- 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.