BIOS Update Release Notes

PRODUCTS: LAPAC71G, LAPAC71H

BIOS Version 0065 - ACADL357.0065.2024.0409.1723

About This Release:

- Date: Apr 09, 2024
- ROM Image Checksum: 0XA60DFF6C
- EC Firmware: 1.12.00.000
- ME Firmware: 16.1.30.2307
- PCH Configuration Firmware: 16.1.0.1014
- PMC Firmware: 160.1.0.1030
- iTBT Firmware: 16.0.0.0202
- IOM Firmware: 36.6.0.0000
- Retimer Firmware in BIOS capsule: 3.9
- NPHY Firmware: 14.531.509.8259
- Platform Properties Assessment Module: 11.22a.7
- CRB Label: ADL_052
- Boot Guard ACM: 1.18.16
- BIOS Guard: BiosGuard_035
- Silicon Initialization Code: Based on 0C.00.69.74
- Memory Reference Code: Based on 0.0.4.60
- Integrated Graphics:
  - UEFI Driver: 21.0.1054
- Intel RST Pre-OS:
  - VMD UEFI Driver: 19.0.0.5428
- Wired LAN Adapter:
  - UEFI Driver: 0.9.03
- AHCI Code: Based on AHCI_30
- 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/Security Patches

- Fixed issue where Flash driver security review
- Fixed issue where UsbRt TOCTOU Vulnerability
- Fixed issue where Vulnerabilities in EDK2 NetworkPkg
- Fixed issue where Extended Image Parser Corruption Correction
- Fixed issue where Image Parser Corruption Vulnerability
- 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 0x433
- Fixed issue where The POST screen is not correct after the BIOS

block downgrade message is displayed.

BIOS Version 0064 - ACADL357.0064.2024.0110.1510

About This Release:

- Date: Jan 10, 2024
- ROM Image Checksum: 0XA6141EDB
- EC Firmware: 1.12.00.000
- ME Firmware: 16.1.27.2176
- PCH Configuration Firmware: 16.1.0.1014
- PMC Firmware: 160.1.0.1029
- iTBT Firmware: 16.0.0.0117
- IOM Firmware: 34.12.0.0000
- Retimer Firmware in BIOS capsule: 3.9
- NPHY Firmware: 14.528.505.8210
- Platform Properties Assessment Module: 11.22a.7
- CRB Label: ADL_052
- Boot Guard ACM: 1.18.15
- BIOS Guard: BiosGuard_035
- Silicon Initialization Code: Based on 0C.00.69.74
- Memory Reference Code: Based on 0.0.4.60
- Integrated Graphics:
  - UEFI Driver: 21.0.1054
- Intel RST Pre-OS:
  - VMD UEFI Driver: 19.0.0.5428
- Wired LAN Adapter:
  - UEFI Driver: 0.9.03
- AHCI Code: Based on AHCI_30
- 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/Security Patches

- Fixed issue where LogoFAIL Vulnerability
- Fixed issue where EDK2 PEI-Phase Denial of Service Vulnerability
- Fixed issue where NetworkPkg EDK2
- Fixed issue where UsbSmmRt vulnerability
- Updated Update Intel KEK/DB keys to support MSFT CA 2023
- Updated CPU Microcode to M80906A3_00000432.pdb

BIOS Version 0063 - ACADL357.0063.2023.1003.1426

About This Release:

- Date: Oct 03, 2023
- ROM Image Checksum: 0XA6293D7C
- EC Firmware: 1.12.00.000

- ME Firmware: 16.1.27.2176
- PCH Configuration Firmware: 16.1.0.1014
- PMC Firmware: 160.1.0.1029
- iTBT Firmware: 16.0.0.0117
- IOM Firmware: 34.12.0.0000
- Retimer Firmware in BIOS capsule: 3.9
- NPHY Firmware: 14.528.505.8210
- Platform Properties Assessment Module: 11.22a.7
- CRB Label: ADL_052
- Boot Guard ACM: 1.18.15
- BIOS Guard: BiosGuard_035
- Silicon Initialization Code: Based on 0C.00.69.74
- Memory Reference Code: Based on 0.0.4.60
- Integrated Graphics:
  - UEFI Driver: 21.0.1054
- Intel RST Pre-OS:
  - VMD UEFI Driver: 19.0.0.5428
- Wired LAN Adapter:
  - UEFI Driver: 0.9.03
- AHCI Code: Based on AHCI_30
- 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/Security Patches

- Fixed issue where TOCTOU Vulnerability in “SmiFlash”.
- Updated CPU Microcode to M80906A3_00000430.pdb.
- Fixed issue where The values of iSetupCfg password check setting are not saved when pressing the SAVE icon in the upper right corner.

BIOS Version 0062 - ACADL357.0062.2023.0724.1432

About This Release:

- Date: July 24, 2023
- ROM Image Checksum: 0XA644BBCA
- EC Firmware: 1.12.00.000
- ME Firmware: 16.1.27.2176
- PCH Configuration Firmware: 16.1.0.1014
- PMC Firmware: 160.1.0.1029
- iTBT Firmware: 16.0.0.0117
- IOM Firmware: 34.12.0.0000
- Retimer Firmware in BIOS capsule: 3.9
- NPHY Firmware: 14.528.505.8210
- Platform Properties Assessment Module: 11.22a.7
- CRB Label: ADL_052
- Boot Guard ACM: 1.18.15

- BIOS Guard: BiosGuard_035
- Silicon Initialization Code: Based on 0C.00.69.74
- Memory Reference Code: Based on 0.0.4.60
- Integrated Graphics:
  - UEFI Driver: 21.0.1054
- Intel RST Pre-OS:
  - VMD UEFI Driver: 19.0.0.5428
- AHCI Code: Based on AHCI_30
- 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/Security Patches

- Updated 2023.3 Intel Platform update.
- Updated support for iFlashV flash tool versions 5.13.00.2106 (X64) / 5.13.00.2106 (Ia32).
- Updated BlackLotus-SecureBoot DBX update.
- Fixed issue where Intel NUC information leak vulnerability.
- Fixed issue where GenericSio Information Disclosure vulnerability.
- Fixed issue where EDK2 vulnerabilities.
- Added PlatformLang Timeout Variable Access.
- Updated OpenSSL Policy Constraints.
- Fixed issue where Heap Buffer Overflow in TCG2MeasurePeImage.
- Updated ADL RC 0C.00.74.20 (3365.00) partial update: Variable buffer overflow.
- Updated Harden SMM Write Flash area.
- Fixed issue where OpenSSL vulnerabilities.
- Updated] ME FW to 16.1.27.2176 (v2).
- Updated CPU Microcode to 0x42C.
- Added "Extend CSME Measurement to TPM-PCR”.
- Fixed issue where When the Intel i219 LAN and Thunderbolt support items are disabled in the BIOS, the system cannot update the BIOS through the Power Button Menu [F7] Flash option.

BIOS Version 0061 - ACADL357.0061.2023.0427.1553

About This Release:

- Date: 04/27/2023
- ROM Image Checksum: 0xA6E91251
- EC Firmware: 1.12.00.000
- ME Firmware: 16.1.25.2124
- PCH Configuration Firmware: 16.1.0.1014
- PMC Firmware: 160.1.0.1029
- iTBT Firmware: 16.0.0.0117
- IOM Firmware: 34.12.0.0000
- Retimer Firmware in BIOS capsule: 3.9
- NPHY Firmware: 14.528.505.8210

- Platform Properties Assessment Module: 11.22a.7
- CRB Label: ADL_052
- Boot Guard ACM: 1.18.12
- Bios Guard: BiosGuard_035
- Silicon Initialization Code: Based on 0C.00.69.74
- Memory Reference Code: Based on 0.0.4.60
- Integrated Graphics:
  - UEFI Driver: 21.0.1054
- Intel RST Pre-OS:
  - VMD UEFI Driver: 19.0.0.5428
- AHCI Code: Based on AHCI_30
- Visual BIOS: Intel AptioV

- Supported Flash Devices:

WinBond	W25Q256FV	32MB
GigaDevice	GD25B256D	32MB

- Microcode Updates included in .BIN & .CAP Files:
  M80906A3_0000042A.pdb

Feature Changes/Updates/Security Patches：

- Updated IPU 2023.1 Update.
- Fixed issue where UEFI Variable access vulnerability.
- Fixed issue where "SmmEntryPoint" Underflow Vulnerability.
- Fixed issue where The Stack Buffer Overflow vulnerability can lead to arbitrary code execution in DXE driver on select Intel platforms.
- Updated ME FW to 16.1.25.2124.
- Updated EC FW to v1.12.00.000
- Updated CPU Microcode to M80906A3_0000042A.pdb

BIOS Version 0060 - ACADL357.0060.2023.0110.1333

About This Release:

- Date: Jan 09, 2023
- ROM Image Checksum: 0xA734ABEF
- EC Firmware: 1.11.00
- ME Firmware: 16.0.15.1810 (v5)
- PCH Configuration Firmware: 16.0.0.1012
- PMC Firmware: 160.01.00.1027
- iTBT Firmware: TBT_ADL_MP_ALL_17.1V1_Rel
- IOM Firmware: 22.000c.0.0000
- Retimer Firmware in BIOS capsule: 3.9
- NPHY Firmware: 14.528.505.8210
- Platform Properties Assessment Module: 11.22a.7
- CRB Label: ADL_052
- Boot Guard ACM: 1.18.10
- Bios Guard: 2.0.5021
- Silicon Initialization Code: Based on 0C.00.69.74
- Memory Reference Code: Based on 0.0.4.60
- Integrated Graphics:
  - UEFI Driver: 21.0.1054

- Intel RST Pre-OS:
  - VMD UEFI Driver: 19.0.0.5428
- AHCI Code: Based on AHCI_30
- Visual BIOS: Intel AptioV

- Supported Flash Devices:

WinBond	W25Q256FV	32MB
GigaDevice	GD25B256D	32MB

- Microcode Updates included in .BIN & .CAP Files:
  M80906A3_00000420.pdb

Feature Changes/Updates/Security Patches：

- Fixed issue where GRUB Bootloader Vulnerability.
- Fixed issue where SIO_DEV_STATUS_VAR_NAME Information Leakage_PTK2712#12.
- Fixed issue where SDIO_DEV_CONFIGURATION SetVariable NVRAM Corruption.
- Updated 2022 IPU update: 2022.3.
- Fixed issue where Intel NUC vulnerability/info leak vulnerability.
- Fixed issue where UEFI Boot Variables Access.
- Fixed issue where TianoCore Security Issues.
- Updated Building Process optimized.
- Updated Changed "Press F8 to Activate Windows Recovery Mode" Boot Flow for "BOOT_FLOW_CONDITION_OEM_KEY3" to "BOOT_FLOW_CONDITION_OEM_KEY4".
- Added BIOS WU setup addition.
- Updated EC FW to v1.11.00
- Fixed issue where OemPL1Time size in stddefault was not correct.

BIOS Version 0059 - ACADL357.0059.2022.1205.2222

About This Release:

- Date: Dec 05, 2022
- ROM Image Checksum: 0xA749E082
- EC Firmware: 1.09.00.000
- ME Firmware: 16.0.15.1810V5
- PCH Configuration Firmware: 16.0.0.1012
- PMC Firmware: 160.01.00.1027
- iTBT Firmware: TBT_ADL_MP_ALL_17.1V1_Rel
- IOM Firmware: 22.000c.0.0000
- Retimer Firmware in BIOS capsule: 3.9
- NPHY Firmware: 14.528.505.8210
- Platform Properties Assessment Module: 11.22a.7
- CRB Label: ADL_052
- Boot Guard ACM: 1.18.10
- Bios Guard: 2.0.5021
- Silicon Initialization Code: Based on 0C.00.69.74
- Memory Reference Code: Based on 0.0.4.6
- Integrated Graphics:
  - UEFI Driver: 21.0.1054

- Intel RST Pre-OS:
  - VMD UEFI Driver: 19.0.0.5428
- AHCI Code: Based on AHCI_30
- Visual BIOS: Intel AptioV

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

- Microcode Updates included in .BIN & .CAP Files:
  M80906A3_00000420.pdb

Feature Change/Updates:

- Fixed issue where Privilege escalation vulnerability from kernel to SMM in multiple devices.
- Fixed issue where Intel NUC information disclosure vulnerability.
- Fixed issue where Potential hack of BIOS EBU DLL.
- Fixed issue where "OpenSSL" (CVE-2022-3786 & CVE-2022-3602) security vulnerabilities.
- Fixed issue where iSetupCfg not able to change default value of PLx/Fan curve parameters due to stdDefault override mechanism.
- Updated Remove Exit button in capsule update page because it is not used.
- Updated Follow RC0C.00.71.76 (3275.00) to revert TME TPM log change.
- Added StdDefaults into ProtectedNvVariableForRuntime ELink.
- Fixed issue where BIOS WU:DF - InfVerif INF Verification-Fails

BIOS Version 0058 - ACADL357.0058.2022.0914.1524

About This Release:

- Date: Sep 14, 2022
- ROM Image Checksum: 0xA74E9909
- EC Firmware: 1.09.00.000
- ME Firmware: 16.0.15.1810V5
- PCH Configuration Firmware: 16.0.0.1012
- PMC Firmware: 160.01.00.1027
- iTBT Firmware: TBT_ADL_MP_ALL_17.1V1_Rel
- IOM Firmware: 22.000c.0.0000
- Retimer Firmware in BIOS capsule: 3.9
- NPHY Firmware: 14.528.505.8210
- Platform Properties Assessment Module: 11.22a.7
- CRB Label: ADL_052
- Boot Guard ACM: 1.18.10
- Bios Guard: 2.0.5021
- Silicon Initialization Code: Based on 0C.00.69.74
- Memory Reference Code: Based on 0.0.4.6
- Integrated Graphics:
  - UEFI Driver: 21.0.1054
- Discrete Graphics:
  - UEFI Driver: 20.1046.0.0
- Intel RST Pre-OS:
  - VMD UEFI Driver: 19.0.0.5428

- AHCI Code: Based on AHCI_30
- Visual BIOS: Intel AptioV

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

- Microcode Updates included in .BIN & .CAP Files:
  M80906A3_00000420.pdb

Feature Change/Update:

- Fixed issue where Windows 11 22H2 WHQL camera related test failure.
- Updated EC FW to v01.09.00

BIOS Version 0055 - ACADL357.0055.2022.0725.2251

About This Release:

- Date: July 25 2022
- ROM Image Checksum: 0xA77F1121
- ME Firmware: 16.0.15.1810 (v5)
- EC Firmware: 1.08.00.000
- PMC Firmware: 160.01.00.1027
- Boot Guard ACM: 1.18.07
- Reference Code: Based on 0C.00.65.70
- Memory Reference Code: Based on 0.0.3.128
- Integrated Graphics:
  - UEFI Driver: 21.0.1054
- Discrete Graphics:
  - UEFI Driver: 20.1046.0.0
- AHCI Code: Based on AHCI_29
- Wired LAN Adapter:
  - UEFI Driver: 0.9.03
- Visual BIOS: Intel AptioV

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

- Microcode Updates included in .BIN & .CAP Files:
  - M80906A3_00000420.pdb

New Fixes/Features:

- Updated ME FW to 16.0.15.1810 (v5)
- Updated EC FW to v1.08.00.000
  For EC 1.08.00.000:
  Improved Thermal performance.
  Improved DC Boot Battery power.
  Improved CPU/GPU Temperature processed.

BIOS Version 0053 - ACADL357.0053.2022.0627.1006

About This Release:

- Date: Jun 27 2022
- ROM Image Checksum: 0xA7852804
- ME Firmware: 16.0.15.1778
- EC Firmware: 1.04.00.000
- PMC Firmware: 160.01.00.1026
- Boot Guard ACM: 1.18.07
- Reference Code: Based on 0C.00.65.70
- Memory Reference Code: Based on 0.0.3.128
- Integrated Graphics:
  - UEFI Driver: 21.0.1046
- AHCI Code: Based on AHCI_29
- Wired LAN Adapter:
  - UEFI Driver: 0.9.03
- Visual BIOS: Intel AptioV

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

- Microcode Updates included in .BIN & .CAP Files:
  - M80906A3_00000420.pdb

New Fixes/Features:

- Initial BIOS version.

LEGAL INFORMATION