CISD BIOS ENGINEERING

Intel Corporation, 5200 NE Elam Young Parkway  
Hillsboro, OR 97124-6497



BIOS Update Release Notes

**Tiger Lake Standard BIOS**

**PRODUCTS**: PATGL357 (Panther Canyon)

### PATGL357.0052.2023.0901.1439 Production BIOS

**About This Release:**

* Date: Aug, 30, 2023
* ROM Image Checksum: 0x9C336434
* EC Firmware: 03.09.00
* ME Firmware: 15.0.42.2411
* PCH Configuration Firmware: 15.0.0.1021
* PMC Firmware: B0 150.1.20.1041
* iTBT Firmware: 15.0.0.4801
* IOM Firmware: 17.24.0.000
* Retimer Firmware in BIOS capsule: NA
* SPHY Firmware: NA
* NPHY Firmware: 11.225.276.2043
* Platform Properties Assessment Module: NA
* I219 NVM: NA
* CRB Label: 5.19\_1AWHY\_RC0A.00.5D.32\_048
* Boot Guard ACM: 1.14.46
* BIOS Guard: BiosGuard\_029
* Silicon Initialization Code: 0A.00.5D.32 (4303.02)
* Memory Reference Code: Based on 2.0.2.8
* MEBx Revision: NA
* Integrated Graphics
  + - Option ROM: NA
    - UEFI Driver: 17.0.1070
* Intel RST Pre-OS
  + - VMD UEFI Driver: 18.1.1.5201
* SATA RAID Option ROM: UEFI Driver : 18.0.5.5115
* SATA non-RAID Option ROM: NA
* AHCI Code: Based on AHCI\_24
* LAN Option ROM: 0.9.03
* Supported Flash Devices:

MACRONIX MX25L25673GM2I-08G 32MB

Winbond W25R256JV 32MB

MX77L25650F

GD25R256D

* Microcode Updates included in .ROM File:

M80806C1\_000000AE.pdb

* Additional Microcode Updates included only in .CAP File:

M80806C1\_000000AE.pdb

**Security patch:**

1. 756386 [Intel/NUC-G][ECS][PA][IPU] IPU 2023.2 update

2. 759664 [Intel/NUC-G][ECS][PA][SA50179/CVE] EDK2 Vulnerabilities

3. 759818 [Intel/NUC-G][ECS][PA][SA50186] OpenSSL Vulnerabilities

4. 759820 [Intel/NUC-G][ECS][PA][SA50158] PlatformLang Timeout Variable Access

5. 759893 [Intel/NUC-G][ECS][PA][PTK3727/SA50093] OOB RW Vulnerabilitity In Intel NUC NUC8i5INH

6. 759894 [Intel/NUC-G][ECS][PA][PTK3725/SA50121] TOCTOU Vulnerabilitity In Intel NUC NUC8i5INH

7. 759896 [Intel/NUC-G][ECS][PA][PTK3596][Utility] Update iFlashV 5.13.00.2106(X64)/5.13.00.2106(Ia32)

8. 759918 [Intel/NUC-G][ECS][PA][SA50193] OpenSSL Policy Constraints

9. 760077 [Intel/NUC-G][ECS][PA][PTK3750/PTK3756][SA50198] Heap Buffer Overflow in TCG2MeasurePeImage

10. 760078 [Intel/NUC-G][ECS][PA][IPU][SA50184] 2023.3 Intel Platform Update

11. 760079 [Intel/NUC-G][ECS][PA][SA50197] BlackLotus-SecureBoot DBX Update

12. 761982 [Intel/NUC-G][ECS][PA][SA50183] Harden SMM Write Flash

**INT change:**

1. 760080 [Intel/NUC-G][ECS][PA] 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] option.

2. 760081 [Intel/NUC-G][ECS][PA] Check EC version on SMBIOS

**Known Errata:**

1. **It can only be used on FAB-B (FAB-C) boards.**

**Can’t update with previous BIOS (PA0000-PA0031).**

**PA0000-PA0013 for FAB-A only.**

**PA0020-PA0038 for FAB-B (FAB-C)only.**

1. **Cannot use FPT update BIOS after PA0032**
2. **Block downgrade to PA0042(PA0000 ~ PA0042) due to CRB update and support PA lite sku**
3. **Please make sure that the amigendrv64.sys in the system has been deleted before you can execute a new EBU update**

### PATGL357.0051.2023.0420.1005 Production BIOS

**About This Release:**

* Date: April, 21, 2023
* ROM Image Checksum: 0x2F53
* EC Firmware: 03.09.00
* ME Firmware: 15.0.42.2384
* PCH Configuration Firmware: 15.0.0.1021
* PMC Firmware: B0 150.1.20.1041
* iTBT Firmware: 15.0.0.4703
* IOM Firmware: 17.24.0.000
* Retimer Firmware in BIOS capsule: NA
* SPHY Firmware: NA
* NPHY Firmware: 11.225.276.2043
* Platform Properties Assessment Module: NA
* I219 NVM: NA
* CRB Label: 5.19\_1AWHY\_RC0A.00.5D.32\_048
* Boot Guard ACM: 1.14.46
* BIOS Guard: BiosGuard\_029
* Silicon Initialization Code: 0A.00.5D.32 (4303.02)
* Memory Reference Code: Based on 2.0.2.8
* MEBx Revision: NA
* Integrated Graphics
  + - Option ROM: NA
    - UEFI Driver: 17.0.1070
* Intel RST Pre-OS
  + - VMD UEFI Driver: 18.1.1.5201
* SATA RAID Option ROM: UEFI Driver : 18.0.5.5115
* SATA non-RAID Option ROM: NA
* AHCI Code: Based on AHCI\_24
* LAN Option ROM: 0.9.03
* Supported Flash Devices:

MACRONIX MX25L25673GM2I-08G 32MB

Winbond W25R256JV 32MB

MX77L25650F

GD25R256D

* Microcode Updates included in .ROM File:

M80806C1\_000000A6.pdb

* Additional Microcode Updates included only in .CAP File:

M80806C1\_000000A6.pdb

**Security Patch:**

1. [EIP 731735] [Intel/NUC-G][ECS][PA][SA50148] SDIO\_DEV\_CONFIGURATION SetVariable NVRAM Corruption
2. [EIP 731736] [Intel/NUC-G][ECS][PA][PTK2712/SA50175] UEFI Variable access vulnerability
3. [EIP 735908] [Intel/NUC-G][ECS][PA][SA50170] SmmEntryPoint Underflow Vulnerability
4. [EIP 740916] [Intel/NUC-G][ECS][PA][IPU] 2023.1 update

**Feature Change/Update:**

Based on PA0050

1. [EIP None] Update ME to 15.0.42.2384

**Issue Fix:**

1. [EIP 737760] [Intel/NUC-G][ECS][PA] Boot option disappear IPv4 & IPv6 , after setting Network Boot to UEFI PXE & iSCSI.
2. [EIP 737759] [Intel/NUC-G][ECS][PA] F4 BIOS recovery can’t catch BIOS file from USB Device(Type-C port), caused no function

**Known Errata:**

1. **It can only be used on FAB-B (FAB-C) boards.**

**Can’t update with previous BIOS (PA0000-PA0031).**

**PA0000-PA0013 for FAB-A only.**

**PA0020-PA0038 for FAB-B (FAB-C)only.**

1. **Cannot use FPT update BIOS after PA0032**
2. **Block downgrade to PA0042(PA0000 ~ PA0042) due to CRB update and support PA lite sku**
3. **Please make sure that the amigendrv64.sys in the system has been deleted before you can execute a new EBU update**

### PATGL357.0050.2022.1228.1726 Production BIOS

**About This Release:**

* Date: January, 06, 2023
* ROM Image Checksum: 0xBFE1
* EC Firmware: 03.09.00
* ME Firmware: 15.0.35.1898
* PCH Configuration Firmware: 15.0.0.1021
* PMC Firmware: B0 150.1.20.1039
* iTBT Firmware: 14.0.0.4301
* IOM Firmware: 17.21.0.000
* Retimer Firmware in BIOS capsule: NA
* SPHY Firmware: NA
* NPHY Firmware: 11.255.256.2041
* Platform Properties Assessment Module: NA
* I219 NVM: NA
* CRB Label: 1AWHY048
* Boot Guard ACM: 1.14.39
* BIOS Guard: BiosGuard\_029
* Silicon Initialization Code: 0A.00.5D.32 (4303.02)
* Memory Reference Code: Based on 2.0.2.8
* MEBx Revision: NA
* Integrated Graphics
  + - Option ROM: NA
    - UEFI Driver: 17.0.1070
* Intel RST Pre-OS
  + - VMD UEFI Driver: 18.1.1.5201
* SATA RAID Option ROM: UEFI Driver : 18.0.5.5115
* SATA non-RAID Option ROM: NA
* AHCI Code: Based on AHCI\_24
* LAN Option ROM: 0.9.02
* Supported Flash Devices:

MACRONIX MX25L25673GM2I-08G 32MB

Winbond W25R256JV 32MB

MX77L25650F

GD25R256D

* Microcode Updates included in .ROM File:

M80806C1\_000000A6.pdb

* Additional Microcode Updates included only in .CAP File:

M80806C1\_000000A6.pdb

**Security Patch:**

1. [EIP 680837] [Intel/NUC-G][ECS][PA][TGL][PTK1433] PEI memory corruption on server boards and on majority of NUCs
2. [EIP 684920] [Intel/NUC-G][ECS][PA][TGL][PTK2427] The stack buffer overflow vulnerability leads to arbitrary code execution in DXE driver on Intel
3. [EIP 685684] [Intel/NUC-G][ECS][PA][TGL][PTK2425] Buffer overflow in UEFI Firmware BIOS core
4. [EIP 688662] [Intel/NUC-G][ECS][PA][TGL][PTK2702] Arbitrary write vulnerability in PEI module leads to arbitrary code execution in PEI phase
5. [EIP 689876] [Intel/NUC-G][ECS][PA][TGL][PTK2699] Information disclosure vulnerability
6. [EIP 690956] [Intel/NUC-G][ECS][PA][TGL][PTK2793] Intel NUC information leak vulnerability
7. [EIP 694614] [Intel/NUC-G][ECS][PA][TGL][PTK2703] The arbitrary code execution in DXE driver
8. [EIP 696359] [Intel/NUC-G][ECS][PA][TGL][PTK2617] SMM memory corruption vulnerability in SMM driver on Intel platforms
9. [EIP 697894] [Intel/NUC-G][ECS][PA][PTK2778] Stack overflow vulnerability in SMI handler
10. [EIP 701859] [Intel/NUC-G][ECS][PA][PTK2911/SA50133] RSB Stuffing Mitigation for Speculative Execution Vulnerability
11. [EIP 701944] [Intel/NUC-G][ECS][PA][SA50085] Grub Bootloader Vulnerability
12. [EIP 701805] [Intel/NUC-G][ECS][PA][TGL][PTK2712-CRB/OEM] UEFI Variable access vulnerability in Intel NUC BIOS
13. [EIP 707144] [Intel/NUC-G][ECS][PA][PTK2712/SA50151] SIO\_DEV\_STATUS\_VAR\_NAME Information Leakage\_PTK2712
14. [EIP 707912] [Intel/NUC-G][ECS][PA][PTK2872] Potential hack of EBU DLL
15. [EIP 695604] [Intel/NUC-G][ECS][PA][SA50120] BootPerformanceTable\_pointer
16. [EIP 711020] [Intel/NUC-G][ECS][PA][Security][TGL] Implement S3 reboot code in MS support project
17. [EIP 711623] [Intel/NUC-G][ECS][PA][PTK2696] Intel NUC information disclosure vulnerability
18. [EIP None] Update MCU to M80806C1\_000000A6
19. [EIP 713440] [Intel/NUC-G][ECS][PA][SA50088] TianoCore Security Issues
20. [EIP 713474] [Intel/NUC-G][ECS][PA][PTK2828/PTK2829] Intel NUC 8 vulnerability/Intel NUC 8 info leak vulnerability
21. [EIP 712642] [Intel/NUC-G][ECS][PA][IPU] 2022 IPU update: 2022.1/2022.2/2022.3
22. [EIP 721838] [Intel/NUC-G][ECS][PA][PTK2975] OS Kernel-level malware may cause information disclosure vulnerability
23. [EIP 724399] [Intel/NUC-G][ECS][PA][SA50157] UEFI Boot Variables Access

**Feature Change/Update:**

Based on PA0048

1. [EIP 707291] [Intel/NUC-G][ECS][PA] Added Test EC FW for TBT P2P issue to build ESA DBIOS.
2. [EIP 703651] [Intel/NUC-G][ECS][PA] POST hotkey message no show w/ Secure Boot enabled.
3. [EIP 712838] [Intel/NUC-G][ECS][PA] Enable TCO timer standard token
4. [EIP 712846] [Intel/NUC-G][ECS][PA] BIOS Warning message during BIOS WU
5. [EIP 712859] [Intel/NUC-G][ECS][PA] Correct EC MMIO Driver (ACPI memory resource RangeLength) to 0x100
6. [EIP 712840] [Intel/NUC-G][ECS][PA] Patch of BIOS warning message for BIOS roll back flash block
7. [EIP 712865] [Intel/NUC-G][ECS][PA] Layout the F6 string to optimize the symptom that caused by Pressing F6 exit MFG.
8. [EIP 713971] [Intel/NUC-G][ECS][PA] Variable Struct Counter
9. [EIP 721312] [Intel/NUC-G][ECS][PA] Add StdDefaults into ProtectedNvVariableForRuntime ELink.
10. [EIP 722750] [Intel/NUC-G][ECS][PA] Add BIOS WU Support
11. [EIP 724028] [Intel/NUC-G][ECS][PA] Building Process optimize\_avoid UQI duplicated

**Issue Fix:**

1. [EIP 699662] [Intel/NUC-G][ECS][PA] Displaying the ENERGY STAR logo in the BIOS setup page when enabled HDD password of the L10 SKU
2. [EIP 712850] [Intel/NUC-G][ECS][PA] Fix ME minor version checking algorithm
3. [EIP 712848] [Intel/NUC-G][ECS][PA] BIOS RTC Reset feature causes BIOS recovery dead loop
4. [EIP 712856] [Intel/NUC-G][ECS][PA] fTPM lost after RTC reset
5. [EIP 712866] [Intel/NUC-G][ECS][PA][Tool] ISetupCfg Tool to modify power limit value, not change.
6. [EIP 721311] [Intel/NUC-G][ECS][PA] With admin password set and User Access Level configured POST Hotkeys, POST hotkey F8 should not pop up the password prompt.
7. [EIP 721914] [Intel/NUC-G][ECS][PA] iSetupCfg tool shows the unexpected message, “WARNING: Duplicate questions”

**Known Errata:**

1. **It can only be used on FAB-B (FAB-C) boards.**

**Can’t update with previous BIOS (PA0000-PA0031).**

**PA0000-PA0013 for FAB-A only.**

**PA0020-PA0038 for FAB-B (FAB-C)only.**

1. **Cannot use FPT update BIOS after PA0032**
2. **Block downgrade to PA0042(PA0000 ~ PA0042) due to CRB update and support PA lite sku**
3. **Please make sure that the amigendrv64.sys in the system has been deleted before you can execute a new EBU update**
4. **PA Lite SKU can’t update ME via jumper recovery.**

### PATGL357.0049.2022.1102.1046 Dropped BIOS

**About This Release:**

* Date: November, 04, 2022
* ROM Image Checksum: 0x4032
* EC Firmware: 03.09.00
* ME Firmware: 15.0.41.2142
* PCH Configuration Firmware: 15.0.0.1021
* PMC Firmware: B0 150.1.20.1041
* iTBT Firmware: 15.0.0.4501
* IOM Firmware: 17.23.0.000
* Retimer Firmware in BIOS capsule: 2.17
* SPHY Firmware: NA
* NPHY Firmware: 11.255.276.2042
* Platform Properties Assessment Module: NA
* I219 NVM: NA
* CRB Label: 1AWHY048
* Boot Guard ACM: 1.14.25
* BIOS Guard: BiosGuard\_029
* Silicon Initialization Code: 0A.00.5D.32 (4303.02)
* Memory Reference Code: Based on 2.0.2.8
* MEBx Revision: NA
* Integrated Graphics
  + - Option ROM: NA
    - UEFI Driver: 17.0.1070
* Intel RST Pre-OS
  + - VMD UEFI Driver: 18.1.1.5201
* SATA RAID Option ROM: UEFI Driver : 18.0.5.5115
* SATA non-RAID Option ROM: NA
* AHCI Code: Based on AHCI\_24
* LAN Option ROM: 0.9.02
* Supported Flash Devices:

MACRONIX MX25L25673GM2I-08G 32MB

Winbond W25R256JV 32MB

MX77L25650F

GD25R256D

* Microcode Updates included in .ROM File:

M80806C1\_000000A6.pdb

* Additional Microcode Updates included only in .CAP File:

M80806C1\_000000A6.pdb

**Security Patch:**

1. [EIP 680837] [Intel/NUC-G][ECS][PA][TGL][PTK1433] PEI memory corruption on server boards and on majority of NUCs
2. [EIP 684920] [Intel/NUC-G][ECS][PA][TGL][PTK2427] The stack buffer overflow vulnerability leads to arbitrary code execution in DXE driver on Intel
3. [EIP 685684] [Intel/NUC-G][ECS][PA][TGL][PTK2425] Buffer overflow in UEFI Firmware BIOS core
4. [EIP 688662] [Intel/NUC-G][ECS][PA][TGL][PTK2702] Arbitrary write vulnerability in PEI module leads to arbitrary code execution in PEI phase
5. [EIP 689876] [Intel/NUC-G][ECS][PA][TGL][PTK2699] Information disclosure vulnerability
6. [EIP 690956] [Intel/NUC-G][ECS][PA][TGL][PTK2793] Intel NUC information leak vulnerability
7. [EIP 694614] [Intel/NUC-G][ECS][PA][TGL][PTK2703] The arbitrary code execution in DXE driver
8. [EIP 696359] [Intel/NUC-G][ECS][PA][TGL][PTK2617] SMM memory corruption vulnerability in SMM driver on Intel platforms
9. [EIP 697894] [Intel/NUC-G][ECS][PA][PTK2778] Stack overflow vulnerability in SMI handler
10. [EIP 701859] [Intel/NUC-G][ECS][PA][PTK2911/SA50133] RSB Stuffing Mitigation for Speculative Execution Vulnerability
11. [EIP 701944] [Intel/NUC-G][ECS][PA][SA50085] Grub Bootloader Vulnerability
12. [EIP 701805] [Intel/NUC-G][ECS][PA][TGL][PTK2712-CRB/OEM] UEFI Variable access vulnerability in Intel NUC BIOS
13. [EIP 707144] [Intel/NUC-G][ECS][PA][PTK2712/SA50151] SIO\_DEV\_STATUS\_VAR\_NAME Information Leakage\_PTK2712
14. [EIP 707912] [Intel/NUC-G][ECS][PA][PTK2872] Potential hack of EBU DLL
15. [EIP 695604] [Intel/NUC-G][ECS][PA][SA50120] BootPerformanceTable\_pointer
16. [EIP 711020] [Intel/NUC-G][ECS][PA][Security][TGL] Implement S3 reboot code in MS support project
17. [EIP 711623] [Intel/NUC-G][ECS][PA][PTK2696] Intel NUC information disclosure vulnerability
18. [EIP None] Update MCU to M80806C1\_000000A6

**Feature Change/Update:**

Based on PA0048

1. [EIP 707291] [Intel/NUC-G][ECS][PA] Added Test EC FW for TBT P2P issue to build ESA DBIOS.
2. [EIP 703651] [Intel/NUC-G][ECS][PA] POST hotkey message no show w/ Secure Boot enabled.
3. [EIP 712838] [Intel/NUC-G][ECS][PA] Enable TCO timer standard token
4. [EIP 712846] [Intel/NUC-G][ECS][PA] BIOS Warning message during BIOS WU
5. [EIP 712859] [Intel/NUC-G][ECS][PA] Correct EC MMIO Driver (ACPI memory resource RangeLength) to 0x100
6. [EIP 712840] [Intel/NUC-G][ECS][PA] Patch of BIOS warning message for BIOS roll back flash block
7. [EIP 712865] [Intel/NUC-G][ECS][PA] Layout the F6 string to optimize the symptom that caused by Pressing F6 exit MFG.
8. [EIP None] Update ME to 15.0.41.2142

**Issue Fix:**

1. [EIP 699662] [Intel/NUC-G][ECS][PA] Displaying the ENERGY STAR logo in the BIOS setup page when enabled HDD password of the L10 SKU
2. [EIP 712850] [Intel/NUC-G][ECS][PA] Fix ME minor version checking algorithm
3. [EIP 712848] [Intel/NUC-G][ECS][PA] BIOS RTC Reset feature causes BIOS recovery dead loop
4. [EIP 712856] [Intel/NUC-G][ECS][PA] fTPM lost after RTC reset

**Known Errata:**

1. **It can only be used on FAB-B (FAB-C) boards.**

**Can’t update with previous BIOS (PA0000-PA0031).**

**PA0000-PA0013 for FAB-A only.**

**PA0020-PA0038 for FAB-B (FAB-C)only.**

1. **Cannot use FPT update BIOS after PA0032**
2. **Block downgrade to PA0042(PA0000 ~ PA0042) due to CRB update and support PA lite sku**
3. **Please make sure that the amigendrv64.sys in the system has been deleted before you can execute a new EBU update**
4. **PA Lite SKU can’t update ME via jumper recovery.**

### PATGL357.0048.2022.0801.1148 Development BIOS

**About This Release:**

* Date: August 01, 2022
* ROM Image Checksum: 0xB502
* ME Firmware: 15.0.35.1898
* EC Firmware: 03.08.00
* PMC Firmware: B0 150.01.20.1039
* TBT Retimer Firmware : NA
* Memory Reference Code: Based on RC 0A.00.5D.32
* MEBx Revision: NA
* Integrated Graphics
  + - Option ROM: NA
    - UEFI Driver: 17.0.1070
* SATA RAID Option ROM: UEFI Driver : 18.0.5.5115
* SATA non-RAID Option ROM: NA
* AHCI Code: Based on AHCI\_24
* LAN Option ROM: 0.9.02
* Supported Flash Devices:

MACRONIX MX25L25673GM2I-08G 32MB

Winbond W25R256JV 32MB

MX77L25650F

GD25R256D

* Microcode Updates included in .ROM File:

M80806C1\_0000009a.pdb

* Additional Microcode Updates included only in .CAP File:

M80806C1\_0000009a.pdb

**New Fixes/Features:**

Based on PA0047

1. [EIP 692120] [Intel/NUC-G][ECS][TGL][PA][PTK1931][Generic] Privilege escalation vulnerability from kernel to SMM in multiple devices
2. [EIP NONE] Update EC to 03.08.00

**Changes:**

**Known Errata:**

1. **It can only be used on FAB-B (FAB-C) boards.**

**Can’t update with previous BIOS (PA0000-PA0031).**

**PA0000-PA0013 for FAB-A only.**

**PA0020-PA0038 for FAB-B (FAB-C)only.**

1. **Cannot use FPT update BIOS after PA0032**
2. **Block dowgrade to PA0042(PA0000 ~ PA0042) due to CRB update and support PA lite sku**
3. **Please make sure that the amigendrv64.sys in the system has been deleted before you can execute a new EBU update**
4. **PA Lite SKU can’t update ME via jumper recovery.**

### PATGL357.0047.2022.0627.1120 Development BIOS

**About This Release:**

* Date: June 27, 2022
* ROM Image Checksum: 0xD724
* ME Firmware: 15.0.35.1898
* EC Firmware: 03.07.00
* PMC Firmware: B0 150.01.20.1039
* TBT Retimer Firmware : NA
* Memory Reference Code: Based on RC 0A.00.5D.32
* MEBx Revision: NA
* Integrated Graphics
  + - Option ROM: NA
    - UEFI Driver: 17.0.1070
* SATA RAID Option ROM: UEFI Driver : 18.0.5.5115
* SATA non-RAID Option ROM: NA
* AHCI Code: Based on AHCI\_24
* LAN Option ROM: 0.9.02
* Supported Flash Devices:

MACRONIX MX25L25673GM2I-08G 32MB

Winbond W25R256JV 32MB

MX77L25650F

GD25R256D

* Microcode Updates included in .ROM File:

M80806C1\_0000009a.pdb

* Additional Microcode Updates included only in .CAP File:

M80806C1\_0000009a.pdb

**New Fixes/Features:**

Based on PA0046

1. [EIP NONE] Update EC to 03.07.00
2. [EIP NONE] Modify Xml to Remove redundant SPI id

**Changes:**

**Known Errata:**

1. **It can only be used on FAB-B (FAB-C) boards.**

**Can’t update with previous BIOS (PA0000-PA0031).**

**PA0000-PA0013 for FAB-A only.**

**PA0020-PA0038 for FAB-B (FAB-C)only.**

1. **Cannot use FPT update BIOS after PA0032**
2. **Block dowgrade to PA0042(PA0000 ~ PA0042) due to CRB update and support PA lite sku**
3. **Please make sure that the amigendrv64.sys in the system has been deleted before you can execute a new EBU update**

### PATGL357.0046.2022.0608.1909 Development BIOS

**About This Release:**

* Date: June 8, 2022
* ROM Image Checksum: 0xB358
* ME Firmware: 15.0.35.1898
* EC Firmware: 03.04.00
* PMC Firmware: B0 150.01.20.1039
* TBT Retimer Firmware : NA
* Memory Reference Code: Based on RC 0A.00.5D.32
* MEBx Revision: NA
* Integrated Graphics
  + - Option ROM: NA
    - UEFI Driver: 17.0.1070
* SATA RAID Option ROM: UEFI Driver : 18.0.5.5115
* SATA non-RAID Option ROM: NA
* AHCI Code: Based on AHCI\_24
* LAN Option ROM: 0.9.02
* Supported Flash Devices:

MACRONIX MX25L25673GM2I-08G 32MB

Winbond W25R256JV 32MB

MX77L25650F

GD25R256D

* Microcode Updates included in .ROM File:

M80806C1\_0000009a.pdb

* Additional Microcode Updates included only in .CAP File:

M80806C1\_0000009a.pdb

**New Fixes/Features:**

Based on PA0045

1. [EIP NONE] Display and enable item “HD Audio” in setup.

**Changes:**

**Known Errata:**

1. **It can only be used on FAB-B (FAB-C) boards.**

**Can’t update with previous BIOS (PA0000-PA0031).**

**PA0000-PA0013 for FAB-A only.**

**PA0020-PA0038 for FAB-B (FAB-C)only.**

1. **Cannot use FPT update BIOS after PA0032**
2. **Block dowgrade to PA0042(PA0000 ~ PA0042) due to CRB update and support PA lite sku**
3. **Please make sure that the amigendrv64.sys in the system has been deleted before you can execute a new EBU update**

### PATGL357.0045.2022.0602.0215 Development BIOS

**About This Release:**

* Date: June 2, 2022
* ROM Image Checksum: 0x89FB
* ME Firmware: 15.0.35.1898
* EC Firmware: 03.04.00
* PMC Firmware: B0 150.01.20.1039
* TBT Retimer Firmware : NA
* Memory Reference Code: Based on RC 0A.00.5D.32
* MEBx Revision: NA
* Integrated Graphics
  + - Option ROM: NA
    - UEFI Driver: 17.0.1070
* SATA RAID Option ROM: UEFI Driver : 18.0.5.5115
* SATA non-RAID Option ROM: NA
* AHCI Code: Based on AHCI\_24
* LAN Option ROM: 0.9.02
* Supported Flash Devices:

MACRONIX MX25L25673GM2I-08G 32MB

Winbond W25R256JV 32MB

MX77L25650F

GD25R256D

* Microcode Updates included in .ROM File:

M80806C1\_0000009a.pdb

* Additional Microcode Updates included only in .CAP File:

M80806C1\_0000009a.pdb

**New Fixes/Features:**

Based on PA0044

1. [EIP NONE] Update to Chipsetinit TgpLpB0\_V8 and RST 18.1.1.5201
2. [EIP NONE] Rollback vsccommon.bin version to ME 15.0.10.1447
3. [EIP683595] Add work around to avoid system stop at Windows entry when do BIOS capsule update ME and EC at the same time.
4. [EIP672298] [Intel/NUC-G][ECS][PA] HDMI port no display issues

**Changes:**

**Known Errata:**

1. **It can only be used on FAB-B (FAB-C) boards.**

**Can’t update with previous BIOS (PA0000-PA0031).**

**PA0000-PA0013 for FAB-A only.**

**PA0020-PA0038 for FAB-B (FAB-C)only.**

1. **Cannot use FPT update BIOS after PA0032**
2. **Block dowgrade to PA0042(PA0000 ~ PA0042) due to CRB update and support PA lite sku**
3. **Please make sure that the amigendrv64.sys in the system has been deleted before you can execute a new EBU update**

### PATGL357.0044.2022.0413.1439 Development BIOS

**About This Release:**

* Date: Feb 21, 2022
* ROM Image Checksum: 0x529E
* ME Firmware: 15.0.35.1898
* EC Firmware: 03.04.00
* PMC Firmware: B0 150.01.20.1039
* TBT Retimer Firmware : NA
* Memory Reference Code: Based on RC 0A.00.5D.32
* MEBx Revision: NA
* Integrated Graphics
  + - Option ROM: NA
    - UEFI Driver: 17.0.1070
* SATA RAID Option ROM: UEFI Driver : 18.0.5.5115
* SATA non-RAID Option ROM: NA
* AHCI Code: Based on AHCI\_24
* LAN Option ROM: 0.9.02
* Supported Flash Devices:

MACRONIX MX25L25673GM2I-08G 32MB

Winbond W25R256JV 32MB

MX77L25650F

GD25R256D

* Microcode Updates included in .ROM File:

M80806C1\_0000009a.pdb

* Additional Microcode Updates included only in .CAP File:

M80806C1\_0000009a.pdb

**New Fixes/Features:**

Based on PA0043

1. [EIP665462] [Intel/NUC-C][ECS][PA][05361125] The temperature sign (°C) is not being reflected correctly in the BIOS 0042 - Cooling tab
2. [EIP672295] [Intel/NUC-G][ECS][PA] IGD Primary and Secondary item issue
3. [EIP672669] [Intel/NUC-G][ECS][PA] Type-C no Display
4. [EIP672667] [Intel/NUC-G][ECS][PA] Update GOP 1070 for both Original SKU and Lite SKU
5. [EIP672759] [Intel/NUC-G][ECS][PA] Both Audio DSP and Digital Microphone item are lost
6. [EIP672827] [Intel/NUC-C][ECS][PA] BIOS patch of boot options overflow handling
7. [EIPNone] To implement config mode load safe setting

**Changes:**

**Known Errata:**

1. **It can only be used on FAB-B (FAB-C) boards.**

**Can’t update with previous BIOS (PA0000-PA0031).**

**PA0000-PA0013 for FAB-A only.**

**PA0020-PA0038 for FAB-B (FAB-C)only.**

1. **Cannot use FPT update BIOS after PA0032**
2. **Block dowgrade to PA0042(PA0000 ~ PA0042) due to CRB update and support PA lite sku**
3. **Please make sure that the amigendrv64.sys in the system has been deleted before you can execute a new EBU update**

### PATGL357.0043.2022.0221.1106 Development BIOS

**About This Release:**

* Date: Feb 21, 2022
* ROM Image Checksum: 0xD4E5
* ME Firmware: 15.0.35.1898
* EC Firmware: 03.04.00
* PMC Firmware: B0 150.01.20.1039
* TBT Retimer Firmware : NA
* Memory Reference Code: Based on RC 0A.00.5D.32
* MEBx Revision: NA
* Integrated Graphics
  + - Option ROM: NA
    - UEFI Driver: 17.0.1052
* SATA RAID Option ROM: UEFI Driver : 18.0.5.5115
* SATA non-RAID Option ROM: NA
* AHCI Code: Based on AHCI\_24
* LAN Option ROM: 0.9.02
* Supported Flash Devices:

MACRONIX MX25L25673GM2I-08G 32MB

Winbond W25R256JV 32MB

MX77L25650F

GD25R256D

* Microcode Updates included in .ROM File:

M80806C1\_0000009a.pdb

* Additional Microcode Updates included only in .CAP File:

M80806C1\_0000009a.pdb

**New Fixes/Features:**

Based on PA0042

1. EIP652553 [Intel/NUC-C][ECS][PA] Update for 2021.2 IPU BIOS change
2. EIP658858 [Intel/NUC-G][ECS][PA] PTK1885: Unauthorized modification of UEFI variables could disable the protect mechanism of SMM
3. EIP641329 [SPG-PA][ECS]Audio Codec, HDMI2.1 IC Shortage need support new parts.
4. EIP650554 [Intel/NUC-G][ECS][PA]Support Windows 11 21H2
5. EIP663081 [Intel/NUC-G][ECS][PA] Based on Win11 code to build DBIOS for Lite SKU
6. EIPNONE DBIOS PA8042 solution for NSS issue
7. EIPNONE [Intel/NUC-G] Press F6 from BIOS setup to exit MFG mode

**Changes:**

**Known Errata:**

1. **It can only be used on FAB-B (FAB-C) boards.**

**Can’t update with previous BIOS (PA0000-PA0031).**

**PA0000-PA0013 for FAB-A only.**

**PA0020-PA0038 for FAB-B (FAB-C)only.**

1. **Cannot use FPT update BIOS after PA0032**
2. **Block dowgrade to PA0042(PA0000 ~ PA0042) due to CRB update and support PA lite sku**
3. **Please make sure that the amigendrv64.sys in the system has been deleted before you can execute a new EBU update**

### PATGL357.0042.2021.1213.1702 Development BIOS

**About This Release:**

* Date: Dec 13, 2021
* ROM Image Checksum: 0x1aa9
* ME Firmware: 15.0.10.1447
* EC Firmware: 03.04.00
* PMC Firmware: B0 150.01.20.1028
* TBT Retimer Firmware : NA
* Memory Reference Code: Based on RC 0A.00.38.51
* MEBx Revision: NA
* Integrated Graphics
  + - Option ROM: NA
    - UEFI Driver: 17.0.1052
* SATA RAID Option ROM: UEFI Driver : 18.0.5.5115
* SATA non-RAID Option ROM: NA
* AHCI Code: Based on AHCI\_24
* LAN Option ROM: 0.9.02
* Supported Flash Devices:

MACRONIX MX25L25673GM2I-08G 32MB

Winbond W25R256JV 32MB

MX77L25650F

GD25R256D

* Microcode Updates included in .ROM File:

M80806C1\_0000009a.pdb

* Additional Microcode Updates included only in .CAP File:

M80806C1\_0000009a.pdb

**New Fixes/Features:**

Based on PA0041

1. eip598186 The wake system from S5 (Daily/weekly ..etc) Help Text missing after load default.
2. eip601236 To include secure boot PK and related DB into Aptio project source tree
3. eip605460 Event log for Auto RTC feature
4. eip606763 Implement BiosGuard solution for PEI buffer overflow (PTK1439)
5. eip606779 SMM arbitrary code execution may allow attacker to modify SPI flash and launch the BIOS bootkit PTK1459
6. eip607532 able to achieve arbitrary write in SMRAM save state region
7. eip608424 Update MCU 0x78 (Microcode\_302) or higher for IPU2021.1
8. eip613981 Update for PTK1457: Vulnerable EFI variable read procedure PTK1457
9. eip618316 Pop up warning message to user when transition bios is necessary
10. eip621021 D-BIOS for SA50074 - Bootguard TOCTOU vulnerability
11. eip626264 DBIOS for no boot after the BIOS update via WU
12. eip635091 Linux ACPI BIOS error
13. eip640897 BIOS doesn't disable wireless module completely
14. eip642804 BT device yellow bang when resume from S4.
15. eip644185 Support update HDMI2.1 FW function
16. eip644391 LAN i225 disappear after disabling it in device manager
17. eip645115 HSTI fail on Capsule Rollback Capability info. (For Win11 WA)
18. eip651376 Yellow bang near UCM-UCSI ACPI Device in device manager
19. eipN/A EC firmware spelling error in
20. eipN/A Weird BIOS Message when Recovering BIOS

**Changes:**

**Known Errata:**

1. **It can only be used on FAB-B (FAB-C) boards.**

**Can’t update with previous BIOS (PA0000-PA0031).**

**PA0000-PA0013 for FAB-A only.**

**PA0020-PA0038 for FAB-B (FAB-C)only.**

1. **Cannot use FPT update BIOS after PA0032**
2. **Block dowgrade to PA0037(PA0000 ~ PA0037)**
3. **Please make sure that the amigendrv64.sys in the system has been deleted before you can execute a new EBU update**

### PATGL357.0041.2021.0811.1505 Development BIOS

**About This Release:**

* Date: August 11, 2021
* ROM Image Checksum: 0xCBF8
* ME Firmware: 15.0.10.1447
* EC Firmware: 03.03.00
* PMC Firmware: B0 150.01.20.1028
* TBT Retimer Firmware : NA
* Memory Reference Code: Based on RC 0A.00.38.51
* MEBx Revision: NA
* Integrated Graphics
  + - Option ROM: NA
    - UEFI Driver: 17.0.1052
* SATA RAID Option ROM: UEFI Driver : 18.0.5.5115
* SATA non-RAID Option ROM: NA
* AHCI Code: Based on AHCI\_24
* LAN Option ROM: 0.9.02
* Supported Flash Devices:

MACRONIX MX25L25673GM2I-08G 32MB

Winbond W25R256JV 32MB

MX77L25650F

GD25R256D

* Microcode Updates included in .ROM File:

M80806C1\_00000072.pdb

* Additional Microcode Updates included only in .CAP File:

M80806C1\_00000072.pdb

**New Fixes/Features:**

Based on PA0040

**1. WMI**

**a. [Platform Changes] [None EIP] WMI version 1.27.**

**b.** **[Platform Changes][EIP624675] [Intel-SPG][ECS][PA] DBIOS of update WMI for NSS.**

**2. [AMI Changes] [None EIP] GL9755 PCIe Card Reader BIOS Programming Guide V1.2 2021/03/22.**

**3. [Platform changes][EIP625968] WD Blue SN550 causes BSOD after waking up from MDSB.**

**Changes:**

1. **EIP602373 [Intel-SPG][ECS][PA]Add BIOS / EC SPI Rom to next formal BIOS.**

**You need to use jumper recovery to update ME settings**

**Known Errata:**

1. **It can only be used on FAB-B (FAB-C) boards.**

**Can’t update with previous BIOS (PA0000-PA0031).**

**PA0000-PA0013 for FAB-A only.**

**PA0020-PA0038 for FAB-B (FAB-C)only.**

1. **Cannot use FPT update BIOS after PA0032**
2. **Block dowgrade to PA0037(PA0000 ~ PA0037)**
3. **Please make sure that the amigendrv64.sys in the system has been deleted before you can execute a new EBU update**

### PATGL357.0040.2021.0414.1645 Development BIOS

**About This Release:**

* Date: April 14, 2021
* ROM Image Checksum: 0xB724
* ME Firmware: 15.0.10.1447
* EC Firmware: 03.03.00
* PMC Firmware: B0 150.01.20.1028
* TBT Retimer Firmware : NA
* Memory Reference Code: Based on RC 0A.00.38.51
* MEBx Revision: NA
* Integrated Graphics
  + - Option ROM: NA
    - UEFI Driver: 17.0.1052
* SATA RAID Option ROM: UEFI Driver : 18.0.5.5115
* SATA non-RAID Option ROM: NA
* AHCI Code: Based on AHCI\_24
* LAN Option ROM: 0.9.02
* Supported Flash Devices:

MACRONIX MX25L25673GM2I-08G 32MB

Winbond W25R256JV 32MB

MX77L25650F

GD25R256D

* Microcode Updates included in .ROM File:

M80806C1\_00000072.pdb

* Additional Microcode Updates included only in .CAP File:

M80806C1\_00000072.pdb

**New Fixes/Features:**

Based on PA0039

**1. EIP597872 [Intel-SPG][ECS][PA] Update NTFS\_06 for "Heap corruption and denial of service in NTFS DXE driver in process of parsing NTFS file system partition"**

**2. EIP600696 [Intel-SPG][ECS][PA]Modify Max. DUTY to 100% when change FAN Control Mode item setting to Custom.**

**3. EIP602371 [Intel-SPG][ECS][PA] Power button led set to sw control issue**

**4.Update SPG Module with CRB32 TAG version**

**5. EIP605873 OFBD module SMI handler vulnerabilities**

**6.Remove Retimer FW binary.**

**Changes:**

1. **EIP602373 [Intel-SPG][ECS][PA]Add BIOS / EC SPI Rom to next formal BIOS.**

**You need to use jumper recovery to update ME settings**

**Known Errata:**

1. **It can only be used on FAB-B (FAB-C) boards.**

**Can’t update with previous BIOS (PA0000-PA0031).**

**PA0000-PA0013 for FAB-A only.**

**PA0020-PA0038 for FAB-B (FAB-C)only.**

1. **Cannot use FPT update BIOS after PA0032**
2. **Block dowgrade to PA0037(PA0000 ~ PA0037)**
3. **Please make sure that the amigendrv64.sys in the system has been deleted before you can execute a new EBU update**

### PATGL357.0039.2021.0224.1510 Development BIOS

**About This Release:**

* Date: February 24, 2021
* ROM Image Checksum: 0x0861
* ME Firmware: 15.0.10.1447
* EC Firmware: 03.03.00
* PMC Firmware: B0 150.01.20.1028
* TBT Retimer Firmware : NA
* Memory Reference Code: Based on RC 0A.00.38.51
* MEBx Revision: NA
* Integrated Graphics
  + - Option ROM: NA
    - UEFI Driver: 17.0.1052
* SATA RAID Option ROM: UEFI Driver : 18.0.5.5115
* SATA non-RAID Option ROM: NA
* AHCI Code: Based on AHCI\_24
* LAN Option ROM: 0.9.02
* Supported Flash Devices:

MACRONIX MX25L25673GM2I-08G 32MB

Winbond W25R256JV 32MB

* Microcode Updates included in .ROM File:

M80806C1\_00000072.pdb

* Additional Microcode Updates included only in .CAP File:

M80806C1\_00000072.pdb

**New Fixes/Features:**

Based on PA0038

**1. CRB Setup item "PCH\_SETUP.PchHdaIDisplayLinkTmode" value from "2" to "3"**

**Known Errata:**

1. **It can only be used on FAB-B (FAB-C) boards.**

**Can’t update with previous BIOS (PA0000-PA0031).**

**PA0000-PA0013 for FAB-A only.**

**PA0020-PA0038 for FAB-B (FAB-C)only.**

1. **Cannot use FPT update BIOS after PA0032**
2. **Block dowgrade to PA0037(PA0000 ~ PA0037)**
3. **Please make sure that the amigendrv64.sys in the system has been deleted before you can execute a new EBU update**

### PATGL357.0038.2021.0120.2042 Development BIOS

**About This Release:**

* Date: January 21, 2021
* ROM Image Checksum: 0x244C
* ME Firmware: 15.0.10.1447
* EC Firmware: 03.03.00
* PMC Firmware: B0 150.01.20.1028
* TBT Retimer Firmware : NA
* Memory Reference Code: Based on RC 0A.00.38.51
* MEBx Revision: NA
* Integrated Graphics
  + - Option ROM: NA
    - UEFI Driver: 17.0.1052
* SATA RAID Option ROM: UEFI Driver : 18.0.5.5115
* SATA non-RAID Option ROM: NA
* AHCI Code: Based on AHCI\_24
* LAN Option ROM: 0.9.02
* Supported Flash Devices:

MACRONIX MX25L25673GM2I-08G 32MB

Winbond W25R256JV 32MB

* Microcode Updates included in .ROM File:

M80806C1\_00000072.pdb

* Additional Microcode Updates included only in .CAP File:

M80806C1\_00000072.pdb

**New Fixes/Features:**

Based on PA0037

**1. AMI CRB core base to 5.19\_1AWHY\_RC0A.00.38.51\_032**

**2. ME Version : 15.0.10.1447**

**3. EIP590512 Added TBT retime FW 2.17 to CAP(For Update)**

**4. Microcode to 0x72.**

**5. EIP590511 GOP to 17.0.1052**

**6. WMI Method 09. SPEC 1.27 shows the wrong value. It should be 0x0127.**

**7. EIP566116 BIOS Setup issue via pressing F2 in Secure Jumper**

**8. RST 18.0.5.5115 RST VMD Driver**

**Known Errata:**

1. **It can only be used on FAB-B (FAB-C) boards.**

**Can’t update with previous BIOS (PA0000-PA0031).**

**PA0000-PA0013 for FAB-A only.**

**PA0020-PA0038 for FAB-B (FAB-C)only.**

1. **Cannot use FPT update BIOS after PA0032**
2. **Block dowgrade to PA0037(PA0000 ~ PA0037)**

### PATGL357.0037.2021.0106.1527 Development BIOS

**About This Release:**

* Date: January 06, 2021
* ROM Image Checksum: 0xA9E1
* ME Firmware: 15.0.2.1377
* EC Firmware: 03.03.00
* PMC Firmware: B0 150.01.20.1024
* TBT Retimer Firmware : NA
* Memory Reference Code: Based on RC 0A.00.34.21
* MEBx Revision: NA
* Integrated Graphics
  + - Option ROM: NA
    - UEFI Driver: 17.0.1041
* SATA RAID Option ROM: UEFI Driver : 18.0.1.1138.2
* SATA non-RAID Option ROM: NA
* AHCI Code: Based on AHCI\_24
* LAN Option ROM: 0.8.10
* Supported Flash Devices:

MACRONIX MX25L25673GM2I-08G 32MB

Winbond W25R256JV 32MB

* Microcode Updates included in .ROM File:

M80806C1\_00000068.pdb

* Additional Microcode Updates included only in .CAP File:

M80806C1\_00000068.pdb

**New Fixes/Features:**

Based on PA0035

**1. EIP587355 - Optimize the POST time (Remove PDUpdateInformation)**

**2. EIP587365 - Remove "Display HDMI Port" from BIOS setup.**

**3. EIP587368 - Update EC firmware 3.03**

**4. EIP567147 - BIOS/CIR Remote Controller Type Fail**

**5. EIP584356 - Update power setting for PA i7/i5/i3.**

**6. EIP587369 - Add Selfhealing Feature.**

**7. Fixed Fault Tolerance issue.**

**8. EIP587370 - Increase USB\_DEV\_MASS\_COUNT.**

**9. EIP587372 - IOMT Tool test failed**

**10. F8 hotkey no function on POST**

**11. ME update issue.**

**12. Auto RTC Reset recovery ME issue**

**13. EIP56615 Characters lacked in "BIOS Recovery Complete"prompt information after BIOS Recovery**

**14. T\_ACPI\_OEM\_TBL\_ID**

**15. Assert error a. F9 : Load default b. F10 : Save and Exit**

**16. Avoid retimer f/w update when version is the same.**

**17.** WMI LED : **NewGetLedStatus HDD LED w/ HDD Activity Returning Error 0xE4(228) instead of OnToOff or OffToOn Value**

**Known Errata:**

1. **It can only be used on FAB-B (FAB-C) boards.**

**Can’t update with previous BIOS (PA0000-PA0031).**

**PA0000-PA0013 for FAB-A only.**

**PA0020-PA0037 for FAB-B (FAB-C)only.**

1. **Cannot use FPT update BIOS after PA0032**

### PATGL357.0035.2020.1113.1353 Development BIOS

**About This Release:**

* Date: November 13, 2020
* ROM Image Checksum: 0x8B4C
* ME Firmware: 15.0.2.1377
* EC Firmware: 03.01.00
* PMC Firmware: B0 150.01.20.1024
* TBT Retimer Firmware : NA
* Memory Reference Code: Based on RC 0A.00.34.21
* MEBx Revision: NA
* Integrated Graphics
  + - Option ROM: NA
    - UEFI Driver: 17.0.1041
* SATA RAID Option ROM: UEFI Driver : 18.0.1.1138.2
* SATA non-RAID Option ROM: NA
* AHCI Code: Based on AHCI\_24
* LAN Option ROM: 0.8.10
* Supported Flash Devices:

MACRONIX MX25L25673GM2I-08G 32MB

Winbond W25R256JV 32MB

* Microcode Updates included in .ROM File:

M80806C1\_00000068.pdb

* Additional Microcode Updates included only in .CAP File:

M80806C1\_00000068.pdb

**New Fixes/Features:**

Based on PA0034

1. Add "Wake from Thunderbolt Device" item in PA BIOS and connect to CRB item "VCCST status of IOM"

2. Correct return value for WMI Method 03h.

3. Update Microcode to 0x68

4. [EIP572691] Fixed that the "Unlimited Boot to Network Attempts" item could not work correctly.

5. Memory quantity shows incorrect under OS(Type 17 issue)

**Known Errata:**

1. **It can only be used on FAB-B (FAB-C) boards.**

**Can’t update with previous BIOS (PA0000-PA0031).**

**PA0000-PA0013 for FAB-A only.**

**PA0020-PA0035 for FAB-B (FAB-C)only.**

1. **Cannot use FPT update BIOS after PA0032**

### TGL357.0034.2020.1110.0720 Development BIOS

**About This Release:**

* Date: November 11, 2020
* ROM Image Checksum: 0xECE6
* ME Firmware: 15.0.2.1377
* EC Firmware: 03.01.00
* PMC Firmware: B0 150.01.20.1024
* TBT Retimer Firmware : NA
* Memory Reference Code: Based on RC 0A.00.34.21
* MEBx Revision: NA
* Integrated Graphics
  + - Option ROM: NA
    - UEFI Driver: 17.0.1041
* SATA RAID Option ROM: UEFI Driver : 18.0.1.1138.2
* SATA non-RAID Option ROM: NA
* AHCI Code: Based on AHCI\_24
* LAN Option ROM: 0.8.10
* Supported Flash Devices:

MACRONIX MX25L25673GM2I-08G 32MB

Winbond W25R256JV 32MB

* Microcode Updates included in .ROM File:

M80806C1\_00000066.pdb

* Additional Microcode Updates included only in .CAP File:

M80806C1\_00000066.pdb

**New Fixes/Features:**

Based on PA0033

1. WHQL : Secure Boot Manual Logo Test

2. suppress "SelfHealSupport"

3. Storage D3 support

4. Update core base to 5.19\_1AWHY\_RC0A.00.34.21\_029 and SPG module

5. Setup value, PCH\_SETUP

a. PchHdAudioSndwLinkEnable[0] = 0

b. PchHdAudioSndwLinkEnable[1] = 0

6. Remove TBT retimer FW

7. WHQL : SECURE\_BOOT : "DEFAULT\_SECURE\_BOOT\_DEPLOYED\_MODE" = 1

8. WMI\_CorrectPowerLimit

9. WU fail issue Add setup item "USB Hearder Connector 2"

10. GOP for IGD Primary / Secondary Video Port

11. L10 SKU

a. "RNUC11PAQi70QA",

b. "RNUC11PAQi50WA",

c. "RNUC11PAQi30WA"

12. EC Update for PD FW ,

13. [EIP574206] Thermal trip event/ Power didn`t blink when thermal trip event trigger

14. Refer to the [EIP563724] The Help Text of "Secure Boot" is wrong.

15. FAN Duty Cycle Inc for Cool mode

16. Q15 & Q16

17. Updated EC FW 03.01.00 and coding related to LAN power

18. Please also correct this WMII profile string in the BIOS

19. Remove "Enabled/Dsiabled" "Force Power Pin" in TBT Retimer FW update

20. Added setup item "OemPostLogo"

21. Hidden setup item "TbtSkipPciOprom"

22. Updated uCode : M80806C1\_00000066.pdb

23. ME Pre Lock and FUSE ([PA]Intel\_(R)\_CSME\_15.0.2.1377v2\_B0\_Consumer\_1109.zip)

**Known Errata:**

1. **It can only be used on FAB-B (FAB-C) boards.**

**Can’t update with previous BIOS (PA0000-PA0031).**

**PA0000-PA0013 for FAB-A only.**

**PA0020-PA0034 for FAB-B (FAB-C)only.**

1. **Cannot use FPT update BIOS after PA0032**

### PATGL357.0033.2020.1028.2002 Development BIOS

**About This Release:**

* Date: October 28, 2020
* ROM Image Checksum: 0x519B
* ME Firmware: 15.0.2.1377
* EC Firmware: 02.04.00
* PMC Firmware: B0 150.01.20.1024
* TBT Retimer Firmware : 2.12
* Memory Reference Code: Based on RC 0A.00.2F.30
* MEBx Revision: NA
* Integrated Graphics
  + - Option ROM: NA
    - UEFI Driver: 17.0.1041
* SATA RAID Option ROM: UEFI Driver : 18.0.1.1138.2
* SATA non-RAID Option ROM: NA
* AHCI Code: Based on AHCI\_24
* LAN Option ROM: 0.8.10
* Supported Flash Devices:

MACRONIX MX25L25673GM2I-08G 32MB

Winbond W25R256JV 32MB

* Microcode Updates included in .ROM File:

M80806C1\_00000060.pdb

* Additional Microcode Updates included only in .CAP File:

M80806C1\_00000060.pdb

**New Fixes/Features:**

Based on PA0032

1.      Setup offset issue

2.    Change logo for BIOS guard issue

**Known Errata:**

1. **It can only be used on FAB-B boards.**

**Can’t update with previous BIOS (PA0000-PA0031).**

**PA0000-PA0013 for FAB-A only.**

**PA0020-PA0033 for FAB-B only.**

1. **Cannot use FPT update BIOS after PA0032**

**Can’t update from with previous BIOS (PA0031).**

### PATGL357.0032.2020.1026.0738. Development BIOS

**About This Release:**

* Date: October 26, 2020
* ROM Image Checksum: 0x0AA8
* ME Firmware: 15.0.2.1377
* EC Firmware: 02.04.00
* PMC Firmware: B0 150.01.20.1024
* TBT Retimer Firmware : 2.12
* Memory Reference Code: Based on RC 0A.00.2F.30
* MEBx Revision: NA
* Integrated Graphics
  + - Option ROM: NA
    - UEFI Driver: 17.0.1041
* SATA RAID Option ROM: UEFI Driver : 18.0.1.1138.2
* SATA non-RAID Option ROM: NA
* AHCI Code: Based on AHCI\_24
* LAN Option ROM: 0.8.10
* Supported Flash Devices:

MACRONIX MX25L25673GM2I-08G 32MB

Winbond W25R256JV 32MB

* Microcode Updates included in .ROM File:

M80806C1\_00000060.pdb

* Additional Microcode Updates included only in .CAP File:

M80806C1\_00000060.pdb

**New Fixes/Features:**

Based on PA0031

1.      WMI function for LED

2.      Power setting

1. i3 VCCIN Imax(A) = 65A
2. i3 VCCIN TDC(A) = 43A

3.      Enabled "BiosGuard\_SUPPORT"

4.      EC FW 02.04.00

5.       Power Mode settings

a.    Balanced Enabled

b.    Low Power Enabled

c.    Max Performance Enabled (Default)

7.      Disable WOL as Default

8.      Change new Intel Logo.

9.      Enabled Boot Guard

10.  Updated code for BIOS ReSign

**Known Errata:**

1. **It can only be used on FAB-B boards.**

**Can’t update with previous BIOS (PA0000-PA0031).**

**PA0000-PA0013 for FAB-A only.**

**PA0020-PA0031 for FAB-B only.**

1. **Cannot use FPT update BIOS after PA0032**

**Can’t update from with previous BIOS (PA0031).**

### PATGL357.0031.2020.1016.1129 Development BIOS

**About This Release:**

* Date: October 16, 2020
* ROM Image Checksum: 0x3537
* ME Firmware: 15.0.2.1377
* EC Firmware: 02.03.06
* PMC Firmware: B0 150.01.20.1024
* TBT Retimer Firmware : 2.12
* Memory Reference Code: Based on RC 0A.00.2F.30
* MEBx Revision: NA
* Integrated Graphics
  + - Option ROM: NA
    - UEFI Driver: 17.0.1041
* SATA RAID Option ROM: UEFI Driver : 18.0.1.1138.2
* SATA non-RAID Option ROM: NA
* AHCI Code: Based on AHCI\_24
* LAN Option ROM: 0.8.10
* Supported Flash Devices:

MACRONIX MX25L25673GM2I-08G 32MB

Winbond W25R256JV 32MB

* Microcode Updates included in .ROM File:

M80806C1\_00000060.pdb

* Additional Microcode Updates included only in .CAP File:

M80806C1\_00000060.pdb

**New Fixes/Features:**

Based on PA0030

1. Remove GPP\_B11 setting from OEM GPIO table
2. Updated “AcpiMof.mof” and “WmiMof.asl” for WMI function
3. Updated “PcdTypeCPortsSupported” value from “4” to “2” for UCSI issue
4. Psys PL2 i3 – 84W
5. EC FW : 02.03.06

**Known Errata:**

1. **It can only be used on FAB-B boards.**

**Can’t update with previous BIOS (PA0000-PA0013).**

**PA0000-PA0013 for FAB-A only.**

**PA0020-PA0031 for FAB-B only.**

### PATGL357.0030.2020.1013.2031 Development BIOS

**About This Release:**

* Date: October 13, 2020
* ROM Image Checksum: 0x5139
* ME Firmware: 15.0.2.1377
* EC Firmware: 02.03.03
* PMC Firmware: B0 150.01.20.1024
* TBT Retimer Firmware : 2.12
* Memory Reference Code: Based on RC 0A.00.2F.30
* MEBx Revision: NA
* Integrated Graphics
  + - Option ROM: NA
    - UEFI Driver: 17.0.1041
* SATA RAID Option ROM: UEFI Driver : 18.0.1.1138.2
* SATA non-RAID Option ROM: NA
* AHCI Code: Based on AHCI\_24
* LAN Option ROM: 0.8.10
* Supported Flash Devices:

MACRONIX MX25L25673GM2I-08G 32MB

Winbond W25R256JV 32MB

* Microcode Updates included in .ROM File:

M80806C1\_00000060.pdb

* Additional Microcode Updates included only in .CAP File:

M80806C1\_00000060.pdb

**New Fixes/Features:**

Based on PA0029

1. BKC 38
2. [PA]Intel\_(R)\_CSME\_15.0.2.1377v2\_B0\_Consumer\_1013

**Known Errata:**

1. **It can only be used on FAB-B boards.**

**Can’t update with previous BIOS (PA0000-PA0013).**

**PA0000-PA0013 for FAB-A only.**

**PA0020-PA0030 for FAB-B only.**

1. **Due to ME setting change and the setup structure has new items, it is recommended to use FPT to upgrade to PA0030.**

### PATGL357.0029.2020.1012.0919 Development BIOS

**About This Release:**

* Date: October 12, 2020
* ROM Image Checksum: 0xA832
* ME Firmware: 15.0.1.1345
* EC Firmware: 02.03.03
* PMC Firmware: B0 150.01.20.1022
* Memory Reference Code: Based on RC 0A.00.2F.30
* MEBx Revision: NA
* Integrated Graphics
  + - Option ROM: NA
    - UEFI Driver: 17.0.1041
* SATA RAID Option ROM: UEFI Driver : 18.0.1.1138.2
* SATA non-RAID Option ROM: NA
* AHCI Code: Based on AHCI\_24
* LAN Option ROM: 0.8.10
* Supported Flash Devices:

MACRONIX MX25L25673GM2I-08G 32MB

Winbond W25R256JV 32MB

* Microcode Updates included in .ROM File:

M80806C1\_00000060.pdb

* Additional Microcode Updates included only in .CAP File:

M80806C1\_00000060.pdb

**New Fixes/Features:**

Based on PA0028

1. BKC 38

a. AMI CRB : 5.19\_1AWHY\_RC0A.00.2F.30\_027

b. [PA]intel\_(r)\_csme\_15.0.1.1345v4.2\_b0\_consumer\_0917

c. [PA]tgl-gop-17.0.1045\_0930

1. SMBIOS: Type 0, Type 10, Type 32, Type 41”
2. FIVR Configuration
3. "Retention to Low Current Mode" 0
4. "Retention to High Current Mode" 0
5. "Low to High Current Mode" 0
6. "Off to High Current Mode" 150
7. Setup item
8. "Thunderbolt Support"
9. “HD Audio”
10. “SMBIOS event log”
11. “Intel Platform Trust Technology”
12. [EIP566870] Please remove the Thunderbolt security level.
13. PEGP for MS
14. [EIP534234] CMOS Time fail issue
15. TBT Retimer FW update

**Known Errata:**

1. **It can only be used on FAB-B boards.**

**Can’t update with previous BIOS (PA0000-PA0013).**

**PA0000-PA0013 for FAB-A only.**

**PA0020-PA0029 for FAB-B only.**

1. **Due to ME setting change and the setup structure has new items, it is recommended to use FPT to upgrade to PA0026.**

### PATGL357.0028.2020.0929.1131 Development BIOS

**About This Release:**

* Date: September 29, 2020
* ROM Image Checksum: 0x3816
* ME Firmware: 15.0.2.1377
* EC Firmware: 02.03.00
* PMC Firmware: B0 150.01.20.1024
* Memory Reference Code: Based on RC 0A.00.2D.72
* MEBx Revision: NA
* Integrated Graphics
  + - Option ROM: NA
    - UEFI Driver: 17.0.1041
* SATA RAID Option ROM: UEFI Driver : 18.0.1.1138.2
* SATA non-RAID Option ROM: NA
* AHCI Code: Based on AHCI\_24
* LAN Option ROM: 0.8.10
* Supported Flash Devices:

MACRONIX MX25L25673GM2I-08G 32MB

Winbond W25R256JV 32MB

* Microcode Updates included in .ROM File:

M80806C1\_00000060.pdb

* Additional Microcode Updates included only in .CAP File:

M80806C1\_00000060.pdb

**New Fixes/Features:**

Based on PA0026

1. uCode : Microcode\_288. “M80806C1\_00000060.pdb”
2. DEFAULT\_UCSI\_REV, “0x100”
3. [EIP566492]WOL – disable LAN power
4. Updated code for RTD3 for LAN and set PCIE SSD keep in D0.
5. Add L10 SKU
6. ME FW 15.0.2.1377
7. GOP [PA]tgl-gop-17.0.1044\_0917
8. rst\_pv\_18.0.1.1138.2\_\_pr2
9. [EIP566481]CIR on manufacture mode.

**Known Errata:**

1. **It can only be used on FAB-B boards.**

**Can’t update with previous BIOS (PA0000-PA0013).**

**PA0000-PA0013 for FAB-A only.**

**PA0020-PA0028 for FAB-B only.**

1. **Due to ME setting change and the setup structure has new items, it is recommended to use FPT to upgrade to PA0026.**

### PATGL357.0026.2020.0921.0830 Development BIOS

**About This Release:**

* Date: September 21, 2020
* ROM Image Checksum: 0xF15A
* ME Firmware: 15.0.0.1320
* EC Firmware: 02.03.00
* PMC Firmware: 150.01.20.1020
* Memory Reference Code: Based on RC 0A.00.2D.72
* MEBx Revision: NA
* Integrated Graphics
  + - Option ROM: NA
    - UEFI Driver: 17.0.1041
* SATA RAID Option ROM: UEFI Driver : 18.0.0.1135
* SATA non-RAID Option ROM: NA
* AHCI Code: Based on AHCI\_24
* LAN Option ROM: 0.8.10
* Supported Flash Devices:

MACRONIX MX25L25673GM2I-08G 32MB

Winbond W25R256JV 32MB

* Microcode Updates included in .ROM File:

M80806C1\_00000052.pdb

* Additional Microcode Updates included only in .CAP File:

M80806C1\_00000052.pdb

**New Fixes/Features:**

Based on PA0025

1. AMI CRB code base to “5.19\_1AWHY\_RC0A.00.2D.72\_026”
2. Porting "DisabledorAllowKnownResetPchWdtMethod" for WDT issue
3. Setup item “SATA Controller(s)”
4. For NSS WMI (ACPI device for WMI tool)
5. FIVR setting : CRB setup -> Chipset ->PCH-IO Configuration -> FIVR Configuration.
6. EC FW : "NUC-PA\_v2.3.0\_20200917.bin".
7. ACPI method “ECIB” and “ECMD”
8. [EIP567149]FC-243 Setup Item "M.2 Port 1"
9. [EIP547792] ESA setup issue : Event Log module & user cannot select/click event log item to view it by mouse
10. Remove some setup items

a. "OS Selection"

b. "Expansion Card Text"

**Known Errata:**

1. **It can only be used on FAB-B boards.**

**Can’t update with previous BIOS (PA0000-PA0013).**

**PA0000-PA0013 for FAB-A only.**

**PA0020-PA0026 for FAB-B only.**

1. **Due to ME setting change and the setup structure has new items, it is recommended to use FPT to upgrade to PA0024.**

### PATGL357.0025.2020.0911.1044 Development BIOS

**About This Release:**

* Date: September 11, 2020
* ROM Image Checksum: 0xD641
* ME Firmware: 15.0.0.1320
* EC Firmware: 02.02.00
* PMC Firmware: 150.01.20.1020
* Memory Reference Code: Based on RC 0A.00.2A.30
* MEBx Revision: NA
* Integrated Graphics
  + - Option ROM: NA
    - UEFI Driver: 17.0.1041
* SATA RAID Option ROM: UEFI Driver : 18.0.0.1135
* SATA non-RAID Option ROM: NA
* AHCI Code: Based on AHCI\_24
* LAN Option ROM: 0.8.10
* Supported Flash Devices:

MACRONIX MX25L25673GM2I-08G 32MB

Winbond W25R256JV 32MB

* Microcode Updates included in .ROM File:

M80806C1\_00000052.pdb

* Additional Microcode Updates included only in .CAP File:

M80806C1\_00000052.pdb

**New Fixes/Features:**

Based on PA0024

1. Power Limit setting.
2. WMI Method 603 for PA.
3. Issue Tracker ww37.2 FC-167 [BIOS/USB Header Connector item issue]
4. Issue Tracker ww37.2 FC-168 [BIOS/ "IGD Primary Video Port" / "IGD Secondary Video" item]

Information only, function not ready.

1. PEIM display issue.

Mini DP, Type C hange at CP 0x08

1. [EIP563109] Power LED/ Power LED not blink when system enters into modern standby

Issue tracker ww.37.2 FC-147

1. Remove SATA Controller(s) from Advanced->Storage in BIOS Setup
2. EIP563230 Modern Standby Check Thermal Zones
3. For Q15,Q16 porting
4. [EIP564668] Modify Native ACPI OS PCIe Support item to Enabled.

**Known Errata:**

1. **It can only be used on FAB-B boards.**

**Can’t update with previous BIOS (PA0000-PA0013).**

**PA0000-PA0013 for FAB-A only.**

**PA0020-PA0025 for FAB-B only.**

1. **Due to ME setting change and the setup structure has new items, it is recommended to use FPT to upgrade to PA0024.**

### PATGL357.0024.2020.0904.1158 Development BIOS

**About This Release:**

* Date: September 04, 2020
* ROM Image Checksum: 0xB3C7
* ME Firmware: 15.0.0.1320
* EC Firmware: 02.02.00
* PMC Firmware: 150.01.20.1020
* Memory Reference Code: Based on RC 0A.00.2A.30
* MEBx Revision: NA
* Integrated Graphics
  + - Option ROM: NA
    - UEFI Driver: 17.0.1041
* SATA RAID Option ROM: UEFI Driver : 18.0.0.1135
* SATA non-RAID Option ROM: NA
* AHCI Code: Based on AHCI\_24
* LAN Option ROM: 0.8.10
* Supported Flash Devices:

MACRONIX MX25L25673GM2I-08G 32MB

Winbond W25R256JV 32MB

* Microcode Updates included in .ROM File:

M80806C1\_00000052.pdb

* Additional Microcode Updates included only in .CAP File:

M80806C1\_00000052.pdb

**New Fixes/Features:**

Based on PA0022

1. AMI CRB code base to “5.19\_1AWHY\_RC0A.00.2A.30\_025”
2. ME FW to 15.0.0.1320.
3. GOP EFI driver to 17.0.1042
4. RST EFI driver to 18.0.0.1135
5. USB2 Setting(PortResetMessageEnable)
6. Remove some Cooling page setup items

[BIOS Item / "Internal Ambient Temperature"]

[BIOS Item / "CPU Voltage Regulator Temperature" ]

[BIOS Item / "GPU Voltage Regulator Temperature" ]

[BIOS Item / "DC Input Voltage"]

[BIOS Item / "CPU I/O Voltage"]

[BIOS Item / "GPU Core Voltage"]

1. FC-157 [PA0022 Flash issue] Power on again and monitor will show a white cursor for 5 secs on the left screen before POST appeared

**Known Errata:**

1. **It can only be used on FAB-B boards.**

**Can’t update with previous BIOS (PA0000-PA0013).**

**PA0000-PA0013 for FAB-A only.**

**PA0020-PA0024 for FAB-B only.**

1. **Due to ME setting change and the setup structure has new items, it is recommended to use FPT to upgrade to PA0024.**

### PATGL357.0023.2020.0828.0757 Development BIOS

**About This Release:**

* Date: August 28, 2020
* ROM Image Checksum: 0x141B
* ME Firmware: 15.0.0.1282
* EC Firmware: 02.02.00
* PMC Firmware: 150.01.20.1016
* Memory Reference Code: Based on RC 0A.00.32.2A
* MEBx Revision: NA
* Integrated Graphics
  + - Option ROM: NA
    - UEFI Driver: 17.0.1041
* SATA RAID Option ROM:
* SATA non-RAID Option ROM: NA
* AHCI Code: Based on AHCI\_24
* LAN Option ROM: 0.8.10
* Supported Flash Devices:

MACRONIX MX25L25673GM2I-08G 32MB

Winbond W25R256JV 32MB

* Microcode Updates included in .ROM File:

M80806C1\_0000004E.pdb

* Additional Microcode Updates included only in .CAP File:

M80806C1\_0000004E.pdb

**New Fixes/Features:**

Based on PA0022

1. Modify SDL Token “GC\_Mode0” for display issue(F2,F7,F10).
2. Updated code for LAN wakup in Win10 S5.
3. Updated code for WMI 6.1 Platform Capability Report
4. Updated code for CIR wake up

**Known Errata:**

1. **It can only be used on FAB-B boards.**

**Can’t update with previous BIOS (PA0000-PA0013).**

**PA0000-PA0013 for FAB-A only.**

**PA0020-PA0023 for FAB-B only.**

### PATGL357.0022.2020.0824.1206 Development BIOS

**About This Release:**

* Date: August 24, 2020
* ROM Image Checksum: 0x0129
* ME Firmware: 15.0.0.1282
* EC Firmware: 02.02.00
* PMC Firmware: 150.01.20.1016
* Memory Reference Code: Based on RC 0A.00.32.2A
* MEBx Revision: NA
* Integrated Graphics
  + - Option ROM: NA
    - UEFI Driver: 17.0.1041
* SATA RAID Option ROM:
* SATA non-RAID Option ROM: NA
* AHCI Code: Based on AHCI\_24
* LAN Option ROM: 0.8.10
* Supported Flash Devices:

MACRONIX MX25L25673GM2I-08G 32MB

Winbond W25R256JV 32MB

* Microcode Updates included in .ROM File:

M80806C1\_0000004E.pdb

* Additional Microcode Updates included only in .CAP File:

M80806C1\_0000004E.pdb

**New Fixes/Features:**

Based on PA0021

1. AMI CRB BIOS Label : 5.19\_1AWHY\_RC0A.00.2A.40\_023.
2. HLK USB Exposed Port System Test
3. HLK USB Tpye-C ACPI Validation
4. LAN Power Control

[7] Lan power control. 0h: disable, 1h: enable

1. EC command 0x90 for "EcRecoveryWdtClearRecoveryFlagMethod()"
2. RAID Driver : rst\_pv\_17.9.0.1007\_RaidDriver\_0806
3. Disable LAN function, but system always can wake from LAN.

ECS Issue Tracker ww33.2 FC-086-1

1. EC FW 02.02.00
2. [EIP557185] Please implement the USCI feature on PA FAB-B.

**Known Errata:**

1. **It can only be used on FAB-B boards.**

**Can’t update with previous BIOS (PA0000-PA0013).**

**PA0000-PA0013 for FAB-A only.**

**PA0020-PA0022 for FAB-B only.**

### PATGL357.0021.2020.0810.0740 Development BIOS

**About This Release:**

* Date: August 30, 2020
* ROM Image Checksum: 0x5AD1
* ME Firmware: 15.0.0.1282
* EC Firmware: 02.00.00
* PMC Firmware: 150.01.20.1016
* Memory Reference Code: Based on RC 0A.00.2A.40
* MEBx Revision: NA
* Integrated Graphics
  + - Option ROM: NA
    - UEFI Driver: 17.0.1041
* SATA RAID Option ROM:
* SATA non-RAID Option ROM: NA
* AHCI Code: Based on AHCI\_24
* LAN Option ROM: 0.8.10
* Visual BIOS: NA
* Supported Flash Devices:

MACRONIX MX25L25673GM2I-08G 32MB

Winbond W25R256JV 32MB

* Microcode Updates included in .ROM File:

M80806C1\_0000004E.pdb

* Additional Microcode Updates included only in .CAP File:

M80806C1\_0000004E.pdb

**New Fixes/Features:**

Based on PA0020

1. Updated ME setting (Recommend to use “FPT” or Jumper Recovery to Update BIOS).
2. LAN EFI driver 0.8.10
3. uCode : M80806C1\_0000004E.pdb for FAB-B only
4. [EIP557825]FAN curve table : “PA FAN\_curve\_0805.xlsx”
5. WMI LED function

a. 2.4 New Get LED Status

b. 2.6 Set the value to the control item of the indicator option and the LED type

1. Setup item :
2. FC-124 BIOS item /"CPU Fan Speed" string incorrect"
3. [EIP557534][EIP557535]FC-113 & FC-114 :There are many SATA Port item in Storage page

**Known Errata:**

1. **It can only be used on FAB-B boards.**

**Can’t update with previous BIOS (PA0000-PA0013).**

**PA0000-PA0013 for FAB-A only.**

**PA0020-PA0021 for FAB-B only.**

### PATGL357.0020.2020.0730.1733 Development BIOS

**About This Release:**

* Date: July 30, 2020
* ROM Image Checksum: 0x0D6D
* ME Firmware: 15.0.0.1282
* EC Firmware: 02.00.00
* PMC Firmware: 150.01.20.1016
* Memory Reference Code: Based on RC 0A.00.2A.40
* MEBx Revision: NA
* Integrated Graphics
  + - Option ROM: NA
    - UEFI Driver: 17.0.1041
* SATA RAID Option ROM:
* SATA non-RAID Option ROM: NA
* AHCI Code: Based on AHCI\_24
* LAN Option ROM: NA
* Visual BIOS: NA
* Supported Flash Devices:

MACRONIX MX25L25673GM2I-08G 32MB

Winbond W25R256JV 32MB

* Microcode Updates included in .ROM File:

M80806C1\_0000004C.pdb

* Additional Microcode Updates included only in .CAP File:

M80806C1\_0000004C.pdb

**New Fixes/Features:**

Based on PA00013

1. AMI CRB BIOS Label : 5.19\_1AWHY\_RC0A.00.2A.40\_021
2. Updated ME.
3. EC FW : 02.00.00 (Non-shared ROM)
4. uCode : M80806C1\_0000004C.pdb for FAB-B only

**Known Errata:**

1. **It can only be used on FAB-B boards.**

**Can’t update with previous BIOS (PA0000-PA0013).**

**PA0000-PA0013 for FAB-A only.**

**PA0020 for FAB-B only.**

### PATGL357.0013.2020.0717.0824 Development BIOS

**About This Release:**

* Date: July 17, 2020
* ROM Image Checksum: 0x6A22
* ME Firmware: 15.0.0.1219
* EC Firmware: 01.02.00
* PMC Firmware: 150.1.10.1030
* Memory Reference Code: Based on RC0A.00.28.42
* MEBx Revision: NA
* Integrated Graphics
  + - Option ROM: NA
    - UEFI Driver: 17.0.1037
* SATA RAID Option ROM:
* SATA non-RAID Option ROM: NA
* AHCI Code: Based on AHCI\_23
* LAN Option ROM: NA
* Visual BIOS: NA
* Supported Flash Devices:

MACRONIX MX25L25673GM2I-08G 32MB

Winbond W25R256JV 32MB

* Microcode Updates included in .ROM File:

M80806C0\_00000068.pdb

* Additional Microcode Updates included only in .CAP File:

M80806C0\_00000068.pdb

**New Fixes/Features:**

Based on PA00012

1. Refer to the WMI 1.26, partial method completion
2. 2.3 Query LED Support Capability
3. 2.4 New Get LED Status
4. 2.5 Set an indicator option for the LED type
5. [EIP553600] SD card power state D0 to D3.
6. IO port 0xCF9, 0xE in PEI isssue

**Known Errata:**

1. **It can’t to update with versions prior to PA0009 by CAP file(FNxxxx.cap) , Please use FPT to update.**

**Please refer to the information below.**

1. **ME setting has been changed.**
2. **The ROM layout has been changed.**

### PATGL357.0012.2020.0713.0720 Development BIOS

**About This Release:**

* Date: July 13, 2020
* ROM Image Checksum: 0xF322
* ME Firmware: 15.0.0.1219
* EC Firmware: 01.02.00
* PMC Firmware: 150.1.10.1030
* Memory Reference Code: Based on RC0A.00.28.42
* MEBx Revision: NA
* Integrated Graphics
  + - Option ROM: NA
    - UEFI Driver: 17.0.1037
* SATA RAID Option ROM:
* SATA non-RAID Option ROM: NA
* AHCI Code: Based on AHCI\_23
* LAN Option ROM: NA
* Visual BIOS: NA
* Supported Flash Devices:

MACRONIX MX25L25673GM2I-08G 32MB

Winbond W25R256JV 32MB

* Microcode Updates included in .ROM File:

M80806C0\_00000068.pdb

* Additional Microcode Updates included only in .CAP File:

M80806C0\_00000068.pdb

**New Fixes/Features:**

Based on PA00011

1. [EIP546724] WMI interface v1.25 implementation
2. Refer to the WMI 1.26, partial method completion

Method 601 :

Method 602 : for FAB-A

**Known Errata:**

1. **It can’t to update with versions prior to PA0009 by CAP file(FNxxxx.cap) , Please use FPT to update.**

**Please refer to the information below.**

1. **ME setting has been changed.**
2. **The ROM layout has been changed.**

### PATGL357.0011.2020.0702.1908 Development BIOS

**About This Release:**

* Date: July 02, 2020
* ROM Image Checksum: 0x99B7
* ME Firmware: 15.0.0.1219
* EC Firmware: 01.02.00
* PMC Firmware: 150.1.10.1030
* Memory Reference Code: Based on RC0A.00.28.42
* MEBx Revision: NA
* Integrated Graphics
  + - Option ROM: NA
    - UEFI Driver: 17.0.1037
* SATA RAID Option ROM:
* SATA non-RAID Option ROM: NA
* AHCI Code: Based on AHCI\_23
* LAN Option ROM: NA
* Visual BIOS: NA
* Supported Flash Devices:

MACRONIX MX25L25673GM2I-08G 32MB

Winbond W25R256JV 32MB

* Microcode Updates included in .ROM File:

M80806C0\_00000068.pdb

* Additional Microcode Updates included only in .CAP File:

M80806C0\_00000068.pdb

**New Fixes/Features:**

Based on PA00010

1. AMI CRB BIOS lable: 5.19\_1AWHY\_RC0A.00.28.42\_019
2. Setup page “OnBoard Device”
3. “SDCard 3.0 Controller” Enabled/Disabled
4. "WLAN" is enabled/disabled, this feature can only be turned off in the OS, but we can still see this device in the device manager.
5. Disabled Intel IPCM module
6. Set PchPcieClockUsageOverride[x], PchPcieClkReqSupport[x] for PA Board

X=3 , 4, 5 to Disabled

1. Hide some setup items

a. "Flast Panel"

b. “LED control”

c. "PCIE Bifurcation Configuration"

d. "Power Supply Regulatory"

e. “SMBus connected to PCIe slots”

f. "eMMC Built-in Storage"

g. "Trusted Platform Module 2.0 Presence"

h. "Internal Speaker"

i. “VR Current Limit (ICCmax)(Amps)"

j. "HDMI/DisplayPort Audio"

k. “Display Emulation”

l. “Inconsistent Display Warning”

m. “Internal Graphics”

n."Real-Time Performance Tuning"

**Known Errata:**

1. **It can’t to update with versions prior to PA0009 by CAP file(FNxxxx.cap) , Please use FPT to update.**

**Please refer to the information below.**

1. **ME setting has been changed.**
2. **The ROM layout has been changed.**

### PATGL357.0010.2020.0619.0348 Development BIOS

**About This Release:**

* Date: June 19, 2020
* ROM Image Checksum: 0x5AE2
* ME Firmware: 15.0.0.1219
* EC Firmware: 01.02.00
* PMC Firmware: 150.1.10.1030
* Memory Reference Code: Based on RC0A.00.26.70\_018
* MEBx Revision: NA
* Integrated Graphics
  + - Option ROM: NA
    - UEFI Driver: 17.0.1037
* SATA RAID Option ROM:
* SATA non-RAID Option ROM: NA
* AHCI Code: Based on AHCI\_23
* LAN Option ROM: NA
* Visual BIOS: NA
* Supported Flash Devices:

MACRONIX MX25L25673GM2I-08G 32MB

Winbond W25R256JV 32MB

* Microcode Updates included in .ROM File:

M80806C0\_00000068.pdb

M80806C1\_00000028.pdb

MC2806D0\_00000024.pdb

* Additional Microcode Updates included only in .CAP File:

M80806C0\_00000068.pdb

M80806C1\_00000028.pdb

MC2806D0\_00000024.pdb

**New Fixes/Features:**

Based on PA0009

1. AMI CRB BIOS lable: 5.19\_1AWHY\_RC0A.00.26.70\_018

2. For CRB 18 update,

a. Update ME setting (xml) TopSwapOverride to 256KB for TopSwap2

b. Change ROM Layout

1. [FC-108] [SUT Halt, Post code FF45], when manually change value to

a. IGD minimum memory = 4096MB

b. IGD Aperture size = 1.5GB

1. Disabled CRB setup item “SAGV”
2. [EIP542682] [FC-050] LAN Function normally after disabled in BIOS Setup
3. Updated code for “FAN\_curve\_value\_check\_list-0608\_part2”

**Known Errata:**

1. **It can’t to update with versions prior to PA0009 by CAP file(FNxxxx.cap) , Please use FPT to update.**

**Please refer to the information below.**

1. **ME setting has been changed.**
2. **The ROM layout has been changed.**

### PATGL357.0009.2020.0611.2017 Development BIOS

**About This Release:**

* Date: June 11, 2020
* ROM Image Checksum: 0x21F9
* ME Firmware: 15.0.0.1219
* EC Firmware: 01.02.00
* PMC Firmware: 150.1.10.1030
* Memory Reference Code: Based on RC0A.00.23.51
* MEBx Revision: NA
* Integrated Graphics
  + - Option ROM: NA
    - UEFI Driver: 17.0.1037
* SATA RAID Option ROM:
* SATA non-RAID Option ROM: NA
* AHCI Code: Based on AHCI\_23
* LAN Option ROM: NA
* Visual BIOS: NA
* Supported Flash Devices:

MACRONIX MX25L25673GM2I-08G 32MB

Winbond W25R256JV 32MB

* Microcode Updates included in .ROM File:

M80806C0\_00000068.pdb

M80806C1\_00000028.pdb

MC2806D0\_00000024.pdb

* Additional Microcode Updates included only in .CAP File:

M80806C0\_00000068.pdb

M80806C1\_00000028.pdb

MC2806D0\_00000024.pdb

**New Fixes/Features:**

Based on PA0008

1. PA L10 SKU

i7 L10 SKUs [BXNUC11PAKi7PA], [BXNUC11PAHi7AA], [BXNUC11PAHi7JA]

i5 L10 SKUs [BXNUC11PAKi5PA], [BXNUC11PAHi5JA], [BXNUC11PAHi5CA]

i3 L10 SKUs [BXNUC11PAHi3JA], [BXNUC11PAHi3FA]

For function

a. [F8] Start Windows Recovery Environment (RE)

b. Energy Star Logo Requirement

1. After Power Failure.
2. Enabled “D3ColdEnable”

**Known Errata:**

1. **It can’t to update with versions prior to PA0007 by CAP file(FNxxxx.cap) , Please use FPT to update.**

**Please refer to the information below.**

1. **ME setting has been changed.**
2. **The ROM layout has been changed.**

### PATGL357.0008.2020.0607.2045 Development BIOS

**About This Release:**

* Date: June 7, 2020
* ROM Image Checksum: 0x3751
* ME Firmware: 15.0.0.1219
* EC Firmware: 01.02.00
* PMC Firmware: 150.1.10.1030
* Memory Reference Code: Based on RC0A.00.23.51
* MEBx Revision: NA
* Integrated Graphics
  + - Option ROM: NA
    - UEFI Driver: 17.0.1037
* SATA RAID Option ROM:
* SATA non-RAID Option ROM: NA
* AHCI Code: Based on AHCI\_23
* LAN Option ROM: NA
* Visual BIOS: NA
* Supported Flash Devices:

MACRONIX MX25L25673GM2I-08G 32MB

Winbond W25R256JV 32MB

* Microcode Updates included in .ROM File:

M80806C0\_00000068.pdb

M80806C1\_00000028.pdb

MC2806D0\_00000024.pdb

* Additional Microcode Updates included only in .CAP File:

M80806C0\_00000068.pdb

M80806C1\_00000028.pdb

MC2806D0\_00000024.pdb

**New Fixes/Features:**

Based on PA0007

1. (BKC)WW22
2. ME 15.0.0.1219
3. GOP 17.0.1037
4. pch chipset\_init kit - tglpchlp\_z0v5\_a0v11
5. uCode M80806C0\_00000068.pdb
6. GPIO table, According to TCSS document suggest not re-define the GPIO pin in ODM GPIO table.

Please remove below GPIOs, Thank you!

GPIO\_E18, GPIO\_E19, GPIO\_E20, GPIO\_E21, GPIO\_D9, GPIO\_D10, GPIO\_D11, GPIO\_D12

1. Setup item USB Port Enabled/Disabled/No Detect
2. PA0006 issue

Enabled setup item “PmcLpmS0i3p0En”

1. Enabled/Disabled Setup item "Bluetooth"
2. [EIP542292] Realtek SD card porting.
3. EC share ROM setting for FAB-A
4. [EIP544250] [EIP544252] Blink LED function
5. ControlIommu issue, refer to the EIP538964
6. [EIP543176] EC flash update function not ready. (Separate BIOS/EC SPI ROM design)

Set to disabled for FAB-A board.

**Known Errata:**

1. **It can’t to update with versions prior to PA0007 by CAP file(FNxxxx.cap) , Please use FPT to update.**

**Please refer to the information below.**

1. **ME setting has been changed.**
2. **The ROM layout has been changed.**

### PATGL357.0007.2020.0528.2058 Development BIOS

**About This Release:**

* Date: May 28, 2020
* ROM Image Checksum: 0xCEAD
* ME Firmware: 15.0.0.1192
* EC Firmware: 01.02.03
* PMC Firmware: 150.1.10.1016
* Memory Reference Code: Based on RC0A.00.23.51
* MEBx Revision: NA
* Integrated Graphics
  + - Option ROM: NA
    - UEFI Driver: 17.0.1031
* SATA RAID Option ROM:
* SATA non-RAID Option ROM: NA
* AHCI Code: Based on AHCI\_23
* LAN Option ROM: NA
* Visual BIOS: NA
* Supported Flash Devices:

MACRONIX MX25L25673GM2I-08G 32MB

Winbond W25R256JV 32MB

* Microcode Updates included in .ROM File:

M80806C0\_00000066.pdb

M80806C1\_00000028.pdb

MC2806D0\_00000024.pdb

* Additional Microcode Updates included only in .CAP File:

M80806C0\_00000066.pdb

M80806C1\_00000028.pdb

MC2806D0\_00000024.pdb

**New Fixes/Features:**

Based on PA0006

1. AMI CRB BIOS lable: 5.18\_1AWHY\_RC0A.00.23.51\_017
2. Event Log function:
3. [EIP542316 ] Memory Size Decrease
4. Processor Thermal Trip
5. Remove EC shared ROM settings for issue below

The BIOS update by the CAP file and need to turn off the AC power to work properly

1. Set “GCMode0” value to “800x600” (Refer to the FN) for issue below

FC-060 : [UEFI Shell not display full-screen on HDMI and mini DP port]

1. uCode : AMI label “Microcode\_279”.

a. M80806C0\_00000066.pdb

b. M80806C1\_00000028.pdb

c. MC2806D0\_00000024.pdb

1. [EIP542098] Please follow Intel Modern standby enabling recipe.

**Known Errata:**

1. **The current EC FW 1.2.0 in FAB-A will update the BIOS update by the CAP file and need to turn off the AC power to work properly**
2. **The ROM layout has been changed. It can’t to update with versions prior to PA0006 by CAP file(FNxxxx.cap)**

### PATGL357.0006.2020.0521.2323 Development BIOS

**About This Release:**

* Date: May 21, 2020
* ROM Image Checksum: 0x0B53
* ME Firmware: 15.0.0.1192
* EC Firmware: 01.02.00
* PMC Firmware: 150.1.10.1016
* Memory Reference Code: Based on RC0A.00.22.31
* MEBx Revision: NA
* Integrated Graphics
  + - Option ROM: NA
    - UEFI Driver: 17.0.1031
* SATA RAID Option ROM:
* SATA non-RAID Option ROM: NA
* AHCI Code: Based on AHCI\_23
* LAN Option ROM: NA
* Visual BIOS: NA
* Supported Flash Devices:

MACRONIX MX25L25673GM2I-08G 32MB

Winbond W25R256JV 32MB

* Microcode Updates included in .ROM File:

M80806C0\_00000068.pdb

M80806C1\_00000022.pdb

* Additional Microcode Updates included only in .CAP File:

M80806C0\_00000068.pdb

M80806C1\_00000022.pdb

**New Fixes/Features:**

Based on PA0005

1. SMBIOS

a. Type 0 : EC version

b. Type 3 : Should be changed to 0x23 for MiniPC.

1. Disabled module "SdioDriver".
2. Information in Setup page.

a. LAN MAC Address(Main page)

b. Remove setup Performance->Memory page

c. Remove Graphics Dynamic Frequency display

d. Memory Voltage information in setup Performance page(Read from EC).

1. [EIP542106] Please disable no used ports. (PCIE, SATA, I2C and etc).
2. Setup item "Internal UEFI Shell" function
3. uCode : Microcode\_277.

a. M80806C0\_00000068.pdb

b. M80806C1\_00000022.pdb

1. Add BIOS flash part "Winbond W25R256JV" in ME setting

**Known Errata:**

1. **The current EC FW 1.2.0 in FAB-A will update the BIOS update by the CAP file and need to turn off the AC power to work properly**
2. **Updated "PLATFORM\_GUID" and "FW\_VERSION\_GUID" value to "{CC179F43-D19B-4907-ACB6-90025A56D930}". So it is not possible to update with versions prior to PA0004 by CAP file(FNxxxx.cap)**

### PATGL357.0005.2020.0517.1447 Development BIOS

**About This Release:**

* Date: May 017, 2020
* ROM Image Checksum: 0x9039
* ME Firmware: 15.0.0.1192
* EC Firmware: 01.02.00
* PMC Firmware: 150.1.10.1016
* Memory Reference Code: Based on RC0A.00.22.31
* MEBx Revision: NA
* Integrated Graphics
  + - Option ROM: NA
    - UEFI Driver: 17.0.1031
* SATA RAID Option ROM:
* SATA non-RAID Option ROM: NA
* AHCI Code: Based on AHCI\_23
* LAN Option ROM: NA
* Visual BIOS: NA
* Supported Flash Devices:

MACRONIX MX25L25673GM2I-08G 32MB

* Microcode Updates included in .ROM File:

M80806C0\_00000066.pdb

M80806C1\_00000020.pdb

* Additional Microcode Updates included only in .CAP File:

M80806C0\_00000066.pdb

M80806C1\_00000020.pdb

**New Fixes/Features:**

Based on PA0004

1. Improve AMI CRB Label : “5.18\_1AWHY\_RC0A.00.22.31\_016.1”
2. Improve ESA setup module.
3. [EIP541348] Qi charger module.
4. SMBIOS Type 17 information.
5. Setup item SATA port "DevSlp"

a. SATA Port 0 DevSlp Default value set to "Enabled"

b. SATA Port 1 DevSlp Default value set to "Enabled"

1. Change TBT Security level default value from "1" to "0".
2. [FC-059]Updated code for M.2 NVME information in setup "Advanced" -> "STORAGE" page
3. Updated “PLATFORM\_GUID" & "FW\_VERSION\_GUID", and please refer to the “Known Errata 2”

CC179F43-D19B-4907-ACB6-90025A56D930

1. LED Function for BIOS post.

[EIP534094] [FC-017] HDD LED/ Swap function not ready

[EIP534095] [FC-018] HDD LED/ Indicator Color function not ready.

[EIP534096] [FC-021]Power LED / LED Swap function not ready

[EIP534097] [FC-022] Power LED /LED Indicator Color function not ready

[EIP534098] [FC-023] RGB LED / LED SWAP function not ready

**Known Errata:**

1. **The current EC FW 1.2.0 in FAB-A will update the BIOS update by the CAP file and need to turn off the AC power to work properly**
2. **Updated "PLATFORM\_GUID" and "FW\_VERSION\_GUID" value to "{CC179F43-D19B-4907-ACB6-90025A56D930}". So it is not possible to update with versions prior to PA0004 by CAP file(FNxxxx.cap)**

### PATGL357.0004.2020.0507.1914 Development BIOS

**About This Release:**

* Date: May 07, 2020
* ROM Image Checksum: 0x611B
* ME Firmware: 15.0.0.1192
* EC Firmware: 01.02.00
* PMC Firmware: 150.1.10.1016
* Memory Reference Code: Based on RC0A.00.12.22
* MEBx Revision: NA
* Integrated Graphics
  + - Option ROM: NA
    - UEFI Driver: 17.0.1031
* SATA RAID Option ROM:
* SATA non-RAID Option ROM: NA
* AHCI Code: Based on AHCI\_23
* LAN Option ROM: NA
* Visual BIOS: NA
* Supported Flash Devices:

MACRONIX MX25L25673GM2I-08G 32MB

* Microcode Updates included in .ROM File:

M80806C0\_00000066.pdb

M80806C1\_00000020.pdb

* Additional Microcode Updates included only in .CAP File:

M80806C0\_00000066.pdb

M80806C1\_00000020.pdb

**New Fixes/Features:**

Based on PA0003

1. [EIP539026] : USB S4 wake function
2. FAN Curve Table. “Balanced”, “Fixed”, “Fanless” mode.
3. Setup “Cooling” Page
4. Motherboard Ambient Temperature
5. Memory voltage
6. Processor Input voltage
7. EC FW "NUC-PA\_v1.2.0\_20200504.bin"
8. Board setting
9. PS1, PS2, PS3 BIOS default setting
10. "[SATA]M2\_2280/SATA GEN1,2 TX test Fail"
11. "[USB] High speed Fail : USB\_2, USB31\_1, USB31\_2\_D, USB31\_2\_U
12. Deep sleep function
13. Power Limit function for Setup item
14. Power limit 1
15. Power limit 2
16. Power limit Time
17. Hide setup items, Power page:
18. 1. Sleep type
19. 2. Power sense

**Known Errata:**

### PATGL357.0003.2020.0503.1625 Development BIOS

**About This Release:**

* Date: May 03, 2020
* ROM Image Checksum: 0x58B8
* ME Firmware: 15.0.0.1192
* EC Firmware: 01.01.02
* PMC Firmware: 150.1.10.1016
* Memory Reference Code: Based on RC0A.00.12.22
* MEBx Revision: NA
* Integrated Graphics
  + - Option ROM: NA
    - UEFI Driver: 17.0.1031
* SATA RAID Option ROM:
* SATA non-RAID Option ROM: NA
* AHCI Code: Based on AHCI\_23
* LAN Option ROM: NA
* Visual BIOS: NA
* Supported Flash Devices:

MACRONIX MX25L25673GM2I-08G 32MB

* Microcode Updates included in .ROM File:

M80806C0\_00000066.pdb

M80806C1\_00000020.pdb

* Additional Microcode Updates included only in .CAP File:

M80806C0\_00000066.pdb

M80806C1\_00000020.pdb

**New Fixes/Features:**

Based on PA0002

1. AMI CRB from “5.17\_1AWHY\_RC0A.00.12.17\_014” to “5.18\_1AWHY\_RC0A.00.12.22\_015”
2. FAN Curve Table. “Balanced”, “Fixed”, “Fanless” mode.
3. Setup “Cooling” Page
4. FAN Speed.
5. CPU Temperature
6. PCH Temperature
7. Memory Temperature
8. Motherboard Ambient Temperature
9. Added uCode “M80806C1\_00000020.pdb” for “"Intel(R) Tiger Lake UP3 B-0 Stepping(806C1)"
10. ME Setting form “15.0.0.1166” to “15.0.0.1192”
11. ACPI\_PM\_PROFILE from "2 = Modile" to "1 = Desktop"
12. Disabled Setup item “ControlIommu” for
13. Disabled setup "EnableDptf" will make the system stop CP 0x24

**Known Errata:**

### PATGL579.0002.2020.0423.2140 Development BIOS

**About This Release:**

* Date: April 23, 2020
* ROM Image Checksum: 0xDFC5
* ME Firmware: 15.0.0.1166
* EC Firmware: 01.01.02
* PMC Firmware: 150.1.10.1014
* Memory Reference Code: Based on RC0A.00.12.17\_014
* MEBx Revision: NA
* Integrated Graphics
  + - Option ROM: NA
    - UEFI Driver: 17.0.1031
* SATA RAID Option ROM:
* SATA non-RAID Option ROM: NA
* AHCI Code: Based on AHCI\_23
* LAN Option ROM: NA
* Visual BIOS: NA
* Supported Flash Devices:

MACRONIX MX25L25673GM2I-08G 32MB

* Microcode Updates included in .ROM File:

M80806C0\_00000066.pdb

* Additional Microcode Updates included only in .CAP File:

M80806C0\_00000066.pdb

**New Fixes/Features:**

Based on PA0001

1. PA001 issue
2. Can’t use FPT to flash BIOS.
3. Fixed Yellow bang message on Windows Device Manager
4. Fixed Power button didn't work in OS.
5. EC 0x62/0x66 port issue
6. EC command 0x88, "Notify EC to update BIOS setting to EC NVRAM(e-flash)" in “ReadytoBoot”
7. Updated GPIO setting

{GPIO\_VER2\_LP\_GPP\_E8, {Native2}},

{GPIO\_VER2\_LP\_GPD2, {Native1}},

1. Jump Recovery function, clarify the issue with ECS
2. USB S4/S5 Wakeup
3. [EIP534457] EC flash update function not ready.
4. [EIP534092] [EIP534093 ]For CEC function test
5. Microcode AMI label : \_274, M80806C0\_00000066.pdb
6. [EIP534966] Power setting.
7. H2RAM decode for EC Dx version.
8. Power button menu

**Known Errata:**

### PATGL579.0001.2020.0416.2257 Development BIOS

**About This Release:**

* Date: April 16, 2020
* ROM Image Checksum: 0xCA78
* ME Firmware: 15.0.0.1166
* EC Firmware: 01.01.02
* PMC Firmware: 150.1.10.1014
* Memory Reference Code: Based on RC0A.00.12.17\_014
* MEBx Revision: NA
* Integrated Graphics
  + - Option ROM: NA
    - UEFI Driver: 17.0.1031
* SATA RAID Option ROM:
* SATA non-RAID Option ROM: NA
* AHCI Code: Based on AHCI\_23
* LAN Option ROM: NA
* Visual BIOS: NA
* Supported Flash Devices:

MACRONIX MX25L25673GM2I-08G 32MB

* Microcode Updates included in .ROM File:

M80806C0\_0000005E.pdb

* Additional Microcode Updates included only in .CAP File:

M80806C0\_0000005E.pdb

**New Fixes/Features:**

* Based on AMI TigerLake label: 5.17\_1AWHY\_RC0A.00.12.17\_014

1. Updated code for [EIP534742] [FC-013]BIOS item / USB S4/S5 Power no function
2. Updated code for [EIP534092] [FC-014] HDMI CEC function not ready.

**Known Errata:**

1. **FPT (flash) fail for PA0001**

### PATGL579.0000.2020.0412.1611 Development BIOS

**About This Release:**

* Date: April 12, 2020
* ROM Image Checksum: 0x8CD0
* ME Firmware: 15.0.0.1166
* EC Firmware: 01.01.02
* PMC Firmware: 150.1.10.1014
* Memory Reference Code: Based on RC0A.00.0B.2B
* MEBx Revision: NA
* Integrated Graphics
  + - Option ROM: NA
    - UEFI Driver: 17.0.1031
* SATA RAID Option ROM:
* SATA non-RAID Option ROM: NA
* AHCI Code: Based on AHCI\_22
* LAN Option ROM: NA
* Visual BIOS: NA
* Supported Flash Devices:

MACRONIX MX25L25673GM2I-08G 32MB

* Microcode Updates included in .ROM File:

M80806C0\_0000005E.pdb

* Additional Microcode Updates included only in .CAP File:

M80806C0\_0000005E.pdb

**New Fixes/Features:**

* Based on AMI TigerLake label: (BETA)5.17\_1AWHY\_RC0A.00.0B.2B\_010.

**Known Errata:**

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, lifesaving, 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) 2009 Intel Corporation.