BIOS Release Notes Form

Product Name	**X11DPG-QT**
Release Version	**4.0**
Release Date	**10/26/2023**
Build Date	**07/11/2023**
Previous Version	**3.9**
Update Category	**Critical**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1.[Enhancements] Change BIOS revision to 4.0.** **2.[Enhancements] Update AMI label 5.14_PurleyCrb_0ACLA060 for RC0628.P50 IPU 2023.3 (1). For INTEL-SA-00813 Security Advisory to address CVE-2022-37343(7.2, High), CVE-2022-44611(6.9, Medium), CVE-2022-38083(6.1, Medium), CVE-2022-27879(5.3, Medium) and CVE-2022-43505(4.1, Medium) security issues. (2). For INTEL-SA-00828 Security Advisory to address CVE-2022-40982(6.5, Medium) security issue.** **3.[Enhancements] Update token RC_VERSION_VALUE setting to 628.P50. Update token PRICESSO_0_UCODE_VERSION setting to 02007006. Update token PRICESSO_2_UCODE_VERSION setting to 04003604. Update token PRICESSO_3_UCODE_VERSION setting to 05003604. Update token FW_SPS_VERSION setting to 4.1.5.2.** **4.[Enhancements] Updated Cascade Lake-SP CPU PV microcode for IPU 2023.3.**

	5.[Enhancements] Updated Intel Server Platform Services for Purley Refresh Server Platforms IPU2023.3 4.1.5.2 **6.[Enhancements] Update DBX file for AMI-SA50182 SecureBoot DBX Update**
New features	**1.[Features] Add OutBand/InBand OemFID support.**
Fixes	**1.[Fixes] Fix naming rule for X11DPG 32MB/64MB**

Release Notes from Previous Release(s)

3.9(5/10/2023)

1. [Enhancements] Change BIOS revision to 3.9.
2. [Enhancements] Update AMI label 5.14_PurleyCrb_0ACLA059 for RC0627.P11 IPU 2023.2
(1). For INTEL-SA-00807 Security Advisory to address CVE-2022-38087(4.1, Medium) and CVE-2022-33894(7.5, High) security issues.
3. [Enhancements] Update token RC_VERSION_VALUE setting to 627.P11.
Update token PRICESSO_0_UCODE_VERSION setting to 02006F05.
Update token PRICESSO_1_UCODE_VERSION setting to 03000012.
Update token PRICESSO_2_UCODE_VERSION setting to 04003501.
Update token PRICESSO_3_UCODE_VERSION setting to 05003501.
4. [Enhancements] Updated Cascade Lake-SP CPU PV microcode for IPU 2023.2.

3.8a(12/07/2022)

1.[Enhancements] Update AMI label 5.14_PurleyCrb_0ACLA056 for RC0622.D07 2022.2 IPU. (1). For INTEL-SA-00601 Security Advisory to address CVE-2021-0154(8.2, High), CVE-2021-0153(8.2, High), CVE-2021-33123(8.2, High), CVE-2021-0190(8.2, High), CVE-2021-33122(7.9, High), CVE-2021-33060(7.8, High), CVE-2021-0189(7.5, High), CVE-2021-33124(7.5, High), CVE-2021-33103(7.5, High), CVE-2021-0159(7.4, High), CVE-2021-0188(5.3, Medium) and CVE-2021-0155(4.4, Medium) security issues. (2). For INTEL-SA-00615 Security Advisory to address CVE-2022-21123(6.1, Medium), CVE-2022-21127(5.6, Medium), CVE-2022-21125(5.5, Medium) and CVE-2022-21166(5.5, Medium) security issues. (3). For INTEL-SA-00616 Security Advisory to address CVE-2021-21131(3.3, Low) and CVE-2021-21136(2.7, Low) security issues.
2.[Enhancements] Updated Skylake-SP/Cascade Lake-SP CPU PC microcode for IPU 2022.2. (1). For INTEL-SA-00601 Security Advisory to address CVE-2021-0154(8.2, High), CVE-2021-0153(8.2, High), CVE-2021-33123(8.2, High), CVE-2021-0190(8.2, High), CVE-2021-33122(7.9, High), CVE-2021-33060(7.8, High), CVE-2021-0189(7.5, High), CVE-2021-33124(7.5, High), CVE-2021-33103(7.5, High), CVE-2021-0159(7.4, High), CVE-2021-0188(5.3, Medium) and CVE-2021-0155(4.4, Medium) security issues. (2). For INTEL-SA-00615 Security Advisory to address CVE-2022-21123(6.1, Medium), CVE-2022-21127(5.6, Medium), CVE-2022-21125(5.5, Medium) and CVE-2022-21166(5.5, Medium) security issues. (3). For INTEL-SA-00616 Security Advisory to address CVE-2021-21131(3.3, Low) and CVE-2021-21136(2.7, Low) security issues.

3.[Enhancements] Update token RC_VERSION_VALUE setting to 622.D07. Update token PRICESSO_0_UCODE_VERSION setting to 02006E05. Update token FW_SPS_VERSION setting to 4.1.4.804.
4.[Enhancements] Fix show wrong DIMM location in event log page.
5.[Enhancements] Modify String naming from SMCI to Supermicro.
6.[Enhancements] Remove "Vendor Keys" in security page.
7.[Enhancements] [SMIHandlerSecurityFix] 1.Refine SMM buffer validation in SmmSmbiosELogInitFuncs.c 2.Allocate runtime buffer to trigger ELog SMI in DxeSmmRedirFuncs.c
8.[Enhancements] Update AEP uEFI driver to 01.00.00.3534 for IPU2022.2.
9.[Enhancements] Update BIOS ACM 1.7.54, SINIT ACM 1.7.55 PW for IPU2022.1 to address Intel-TA-00161: CVE-2021-0159 (7.8 High) CVE-2021-33123 (8.2 High) and CVE-2021-33124 (7.5 High)
10.[Enhancements] Update VROC SATA/sSATA legacy driver to VROC PreOS v6.3.5.1003 Hot Fix to fix 10TB or higher volume drive issue.
11.[Enhancements] Update VROC SATA/sSATA EFI driver to VROC PreOS v7.8.0.1012 to address 1. Data Loss Exposure Due to RAID 5 TRIM Support. Document #737276. 2. INTEL-TA-00692. CVE-2022-29919(7.8 High), CVE-2022-30338(6.7 Medium), CVE-2022-29508(6.3 Medium), CVE-2022-25976(5.5 Medium)
12.[Fixes] Enabled IScsi_SUPPORT on Purley generation.
13.[Enhancements] Modify the allocated buffer from EfiBootServicesData to EfiRuntimeServicesData.
14.[Enhancements] Disable MROM1 device since product doesn't use Intel IE function.
15.[Enhancements] Update DBX file to fix Secure Boot Bypass issue.
16.[Enhancements] Update AMI label 5.14_PurleyCrb_0ACLA057 for RC0623.D09 2022.3 IPU. (1) For INTEL-TA-00610 Security Advisory to address CVE-2022-26845 (8.7 High), CVE-2022-27497(8.6 High), CVE-2022-29893 (8.1 High), CVE-2021-33159 (7.4 High), CVE-2022-29466(7.3 High), CVE-2022-29515(6.0 Medium) security issues. (2) For INTEL-TA-00688 Security Advisory to address CVE-2022-26006 (8.2 High), CVE-2022-21198(7.9 High) security issues.
17.[Enhancements] Update token RC_VERSION_VALUE setting to 623.D09. Update token PRICESSO_0_UCODE_VERSION setting to 02006E05. Update token FW_SPS_VERSION setting to 4.1.4.804.
18.[Enhancements] Update Intel DCPM UEFI driver to 1.0.0.3536.
19.[Fixes] Fix OA2 key injection issue.

3.6(01/22/22)
1.[Enhancements] Change BIOS revision to 3.6.
2.[Enhancements] Update SATA/sSATA EFI driver to VROC PreOS v7.7.0.1054.
3.[Enhancements] Update AEP uEFI driver to 1.0.0.3531 for IPU2021.2.
4.[Enhancements] Update AMI label 5.14_PurleyCrb_0ACLA054 for RC0616.D08 2021.2 IPU. For INTEL-SA-00527 Security Advisory to address CVE-2021-0103(8.2, High), CVE-2021-0114(7.9, High), CVE-2021-0115(7.9, High), CVE-2021-0116(7.9,High), CVE-2021-0117(7.9, High), CVE-2021-0118(7.9, High), CVE-2021-0099(7.8, High), CVE-2021-0156(7.5, High), CVE-2021-0111(7.2, High), CVE-2021-0107(7.2, High), CVE-2021-0125(6.7, Medium), CVE-2021-0124(6.3, Medium), CVE-2021-0119(5.8, Medium), CVE-2021-0092(4.7, Medium), CVE-2021-0091(3.2, Low) and CVE-2021-0093(2.4, Low) security issues.
5.[Enhancements] Updated Intel Server Platform Services for Purley Refresh Server Platforms IPU2021.2 HF1 4.1.4.654.6.[Enhancements] Update BIOS ACM 1.7.51, SINIT ACM 1.7.51 PW. For INTEL-SA-00527 Security Advisory to address CVE-2021-0103(8.2, High), CVE-2021-0114(7.9, High), CVE-2021-0115(7.9, High), CVE-2021-0116(7.9, High), CVE-2021-0117(7.9,High), CVE-2021-0118(7.9, High), CVE-2021-0099(7.8, High), CVE-2021-0156(7.5, High), CVE-2021-0111(7.2, High), CVE-2021-0107(7.2, High), CVE-2021-0125(6.7, Medium), CVE-2021-0124(6.3, Medium), CVE-2021-0119(5.8,

Medium), CVE-2021-0092(4.7, Medium), CVE-2021-0091(3.2, Low) and CVE-2021-0093(2.4, Low) security issues.
7.[Enhancements] Updated Skylake-SP/Cascade Lake-SP CPU PV microcode. Updated Skylake-SP H0/M0/U0 stepping CPU PV microcode MB750654_02006C0A. Update Cascade Lake-SP B0 stepping CPU PV microcode MBF50656_0400320A. Update Cascade Lake-SP B1 stepping CPU PV microcode MBF50657_0500320A. For INTEL-SA-00532 Security Advisory to address CVE-2021-0127(5.6, Medium) security issue. For INTEL-SA-00365 Security Advisory to address CVE-2020-8673(4.7,Medium) security issue.

3.5(*05/24/2021*)
1[Enhancements] Update RC 612.D02 for INTEL-SA-00463 Security Advisory to address CVE-2020-12357(7.5, High), CVE-
2020-8670(7.5, High), CVE-2020-8700(7.5, High), CVE-2020-12359(7.1, High), CVE-2020-12358(6.7, Medium), CVE-2020-
12360(5.6, Medium), CVE-2020-24486(5.5, Medium) and CVE-2020-0589(3.8, Low) security issues.
2[Enhancements] Update BIOS ACM 1.7.43, SINIT ACM 1.7.4A PW for INTEL-SA-00463 Security Advisory to address CVE-
2020-12357(7.5, High), CVE-2020-8670(7.5, High), CVE-2020-8700(7.5, High), CVE-2020-12359(7.1, High), CVE-2020-
12358(6.7, Medium), CVE-2020-12360(5.6, Medium), CVE-2020-24486(5.5, Medium) and CVE-2020-0589(3.8, Low)
security issues.
3[Enhancements] Updated Skylake-SP/Cascade Lake-SP CPU PV microcode for INTEL-SA-00464 Security Advisory to
address CVE-2020-24511(5.6, Medium) and CVE-2020-24512(2.8, Low) security issues.
4[Enhancements] Updated Intel Server Platform Services for Purley Refresh Server Platforms 4.1.4.505.
5[Enhancements] Update AEP FW to FW_1.2.0.5446, uEFI driver to 3515 for IPU2021.1.
6[Enhancements] Sync IPv6 status detection rule with BMC to make sure IPv6 status is the same in BIOS and BMC web.

3.4a (03/15/2021)
1. [Enhancements] This system cannot boot into PXE with DVD installed.

3.4 (10/30/2020)
1. Updated 5.14_PurleyCrb_0ACLA052 for RC update and 2020.2 IPU PV to address Intel-TA-00358: CVE-2020-0587 (6.7, Medium), CVE-2020-0591 (6.7, Medium), CVE-2020-0592 (3, Low), and Intel-TA-00390: CVE-2020-0593 (4.7, Medium), CVE-2020-8738 (7.5, High), CVE-2020-8739 (4.6, Medium), CVE-2020-8740 (6.7, Medium), and CVE-2020-8764 (8.7 High) security issues.
2. Updated BIOS ACM 1.7.41 and SINIT ACM 1.7.49 PW to address Intel-TA-00358: CVE-2020-0588 (3.8, Low) and CVE-2020-0590 (7.7, High) security issues.
3. Updated SPS 4.1.4.423 to address Intel-TA-00391: CVE-2020-8755 (4.6, Medium) and CVE-2020-8705 (7.1, High) security issues.
4. Updated Skylake-SP/Cascade Lake-SP CPU PV microcode from 20200918_NDA Release to address Intel-TA-00381: CVE-2020-8696 (2.5, Low) security issue, MD_Clear Errata, MOB Speedpath, and IRR Restore with RS Throttle (ITR #2).
5. Updated SATA/sSATA RAID OPROM/EFI driver to VROC PreOS v6.3.0.1005 PV.
6. Enhanced SMCI HDD Security feature.
7. Added force next boot to UEFI Shell via IPMI support.
8. Added function to move all LANs to the top of boot priority when IPMI forces PXE.
9. Added inband flash status event log to IPMI MEL.

10. Corrected "Station MAC Address" display order when "Configuration Address Source" is set to "Static".
11. Added support for AOC-SHG3-4M2P card sensor reporting in VMD mode.
12. Updated AMI EIP563137 to fix failure of some BIOS items (like boot mode item) to load default with some configurations (like with Micron M.2 or HGST SATA M.2).
13. Fixed failure of "UEFI Compliant - Boot from iSCSI peripheral" in UEFI SCT test.
14. Fixed problem of system hanging during BIOS flash if Watch Dog function is enabled.
15. Fixed inability of 6240R and some refresh 4 serial CPU frequencies to reach maximum when enabling Mwait.
16. Corrected BMC firmware revision in BIOS Setup.
17. Fixed problem of system hanging at 0xB2 with some NVMe devices.
18. Fixed problem of system hanging at POST code 0xA0 or 0xA2 when using unsupported security NVMe device and installing Hyper-V with Windows 2019.

3.3 (02/21/2020)
1. Patched problem of system hanging at 94 with new NVidia RTX 6000/8000.
2. Enabled saving memory CE location into PPR variable at runtime even if memory correctable error reporting is disabled.
3. Added sighting CLX28 workaround and downgraded patrol scrub UC to CE.
4. Added SMC HDD Security feature.
5. Updated AMI label 5.14_PurleyCrb_0ACLA050 beta for IPU2020.1 PV.
6. Updated SPS_E5_04.01.04.381 from IPU 2020.1 PV.
7. Updated BIOS ACM 1.7.40 and SINIT ACM 1.7.48 PW.
8. Added setup item "HDD password prompt Control" to control "Hard-Drive Password Check" for enabling/disabling HDD password prompt window during POST.
9. Updated Skylake-SP/Cascade Lake-SP CPU microcode for Intel-SA-00329 (CVE2020-0548 2.8 Low and CVE2020-0549 6.5 Medium), Intel-SA-00288 (CVE2019-11157 5.3 Medium), and Intel-SA-00317 (CVE2019-14607 7.9 High).
10. Fixed mismatch of Secure Boot Mode value.
11. Removed requirement to use Admin password for erasing TCG device.
12. Fixed problem of two CentOS boot items occurring in boot order if CentOS is installed in RAID 1 system.

3.2 (10/18/2019)
1. Updated Skylake-SP CPU microcode for INTEL-SA-00271 Security Advisory to address CVE-2019-11139 (5.8, Medium) security issue.
2. Updated Cascade Lake-SP CPU microcode for INTEL-SA-00270 Security Advisory to address CVE-2019-11135 (6.5, Medium) security issue.
3. Updated AMI label 5.14_PurleyCrb_0ACLA049 for BKC WW36 and INTEL-SA-00280 to address CVE-2019-11136 (7.5, High) and CVE-2019-11137 (7.5, High) security issues.
4. Updated BIOS ACM 1.7.3 and SINIT ACM 1.7.45 PW from BKC WW36 for INTEL-SA-00240 Security Advisory to address CVE-2019-0151 (7.5, High) and CVE-2019-0152 (8.2, High) security issues.
5. Updated SPS_E5_04.01.04.339.0 from BKC WW36 for INTEL-SA-00241 Security Advisory to address CVE security issues.
6. Updated SATA/sSATA RAID OPROM/EFI driver to VROC PreOS v6.2.0.1034 PV.
7. Updated the behavior for the feature that updates SMBIOS Type 1 and 3 with FRU0.
8. Patched inability of system to boot via onboard LAN2 after IPMI forces PXE boot when there is an OS behind LSI-3108 RAID card.
9. Displayed CPU Flex Ratio-related setup items when the CPU on system supports IntelR Speed Select technology "Performance Profile" feature.

10. Added Redfish/SUM Secure Boot feature and updated OOB for secure boot and reserve Key.
11. Added support for keeping Linux MOK keys database.
12. Added setup item to control 16Gb based Single Die Package DIMM tRFC optimization.
13. Implemented dynamic change for Secure Boot Mode default value.
14. Changed "Secure Boot Mode" to ReadOnly attribute.
15. Added support for firmware version information.
16. Disabled ADDDC/SDDC and set PPR as hPPR.
17. Removed Intel Virtualization Technology override when set to extreme performance.
18. Fixed problem of key details showing "Security Violation" after loading Factory secure boot keys.
19. Fixed failure of the default boot order of UEFI groups to sync when "Boot mode" is under UEFI mode.
20. Fixed problem of two OS (Redhat & Ubuntu) boot devices appearing in boot order.
21. Fixed failure of OPROM control item if CSM is disabled.
22. Fixed inability of onboard VGA to report correct monitor EDID data when secure boot is enabled.
23. Fixed inability to identify duplicate boot options with more than one of the same M.2 AHCI interface devices.
24. Fixed inability of InBand Update BIOS in Linux OS to preserve Linux secureboot keys.
25. Fixed problem of onboard LAN speed dropping from GEN3 to GEN2 during AC on/off testing.

3.1 (05/23/2019)
1. Updated Skylake-SP/Cascade Lake-SP CPU microcode.
2. Updated Intel BKCWW16 2019 PV PLR1.
3. Updated SPS_E5_04.01.04.296.0 from BKC WW16 2019.
4. Updated EIP467272 for AMI SA50069, SA50070.
5. Set SDDC Plus One or SDDC to disabled by default.
6. Updated SATA/sSATA RAID OPROM/EFI driver to VROC PreOS v6.1.0.1017.
7. Set Leaky Bucket that can decrease one memory correctable error count within 2.15 minutes with threshold 512.
8. Corrected hot-plug memory resource assignment of Thunderbolt 2.0 device.
9. Set ADDDC to enabled by default.
10. Fixed problem of system halting or rebooting at POST code 0xB2 or 0x92 when total GPT partition number is more than 256 and RSD is enabled.
11. Fixed problem of "?[1;31;40m" showing on POST screen when EFI driver is "Unhealthy".
12. Fixed inability to change IPv6 address or IPv6 Router1 IP address.
13. Fixed malfunction of workaround for GPU P2P low bandwidth.

3.0c (03/27/2019)
1. Added support for Purley Refresh platform.
2. Enhanced BIOS setup menu to auto-switch the Option ROM's value and hide the unexpected value when boot mode changes.
3. Updated to SPS 4.0.04.381 or above for INTEL-SA-00213 Security Advisory.
4. Fixed problem of UUID showing IPMI MAC incorrectly after disabling onboard LAN chip.
5. Temporarily fixed error for SKX (CLX) 4114 CPU memory training with Micron (18ASF2G72PDZ-2G6E1) RDIMM.
6. Fixed failure to boot into VMware OS when set to Maximum Performance even if Monitor/MWAIT is enabled.

3.0b (03/05/2019)
1. Added support for Purley Refresh platform.
2. Updated CPU microcodes from SRV_P_270.

3. Updated SINIT ACM 1.7.2 PW from BKC WW06 2019.
4. Updated SPS_E5_04.01.04.251.0 from Intel VIP Kit #130885.
5. Added support for Linux built-in utility efibootmgr.
6. Updated IPv6 router-related setup item string.
7. Reduced redundant reboot for offboard VGA switching.
8. Set NVDIMM ADR timeout to 600us.
9. Enabled support for Thunderbolt 2.0.
10. Updated to SPS 4.1.02.174 or above for INTEL-SA-00185 Security Advisory and RC 549.D13 or above for INTEL-SA-00192 Security Advisory.
11. Modified UEFI network description to IPv4/IPv6 to follow Industry Standard.
12. Patched problem of system hanging at 0x94 when plugging in Nvidia Tesla T4 card.
13. Fixed inability of "Network Stack"-related items to get/change via SUM OOB method.

3.0a (12/21/2018)
1. Updated 5.14_PurleyCrb_0ACLA031_BETA for Purley Skylake platform, BKC 2018 WW36.
2. Added support for Monitor Mwait feature.
3. Fixed inability of VMD status to load default if loading default by AFU.
4. Added support for SMC HttpBoot.
5. Fine tuned function code of "Install Windows 7 USB Support" setup item.
6. Removed support for S3 due to SPS ME limitation.
7. Removed support for Thunderbolt.
8. Skipped downgrade of BIOS to 2.x when using next generation CPU.
9. Added support for NVMe auto detection with SMC NVMe add-on card on slot 2/4/6/8/9/10.
10. Added support for Purley Refresh platform.
11. Updated SATA RAID OPROM/EFI driver to RSTe PreOS v6.0.0.1024.
12. Set PCIe correctable and uncorrectable (non-fatal) error report to disabled by default.
13. Set RFC4122 encoding to only be enabled for build time produced by IPMI 1.29 or newer.
14. Updated CPU microcode SRV_P_262 for Skylake-SP H0/M0/U0 CPUs.
15. Disabled unused SPS ME "CUPS IIO" and "Volumetric Airflow" sensor.
16. Fixed problem of BIOS always retrying boot when Re-Try Boot is Disabled.
17. Fixed malfunction of support for LEGACY to EFI.
18. Fixed failure of always turbo in new Linux kernel 7.x.
19. Fixed problem of system hanging and falling into a dead loop when setting enabled CPU core number to 1 in always turbo mode.
20. Fixed problem of CPU core numbers and maximum turbo ratio not matching in always turbo mode.
21. Fixed problem of setup item "Quiet Boot" staying enabled after flashing BIOS with "Quiet Boot" disabled.

2.1 (7/20/2018)
1. Updated CPU microcode to address 'Spectre' derivatives (CVE-2018-3639 & CVE-2018-3640) security issue.
2. Updated Purley RC 154.R13, SPS 4.0.04.340 and ACM 1.3.7, SINIT ACM 1.3.4.
3. Updated SATA RAID OPROM/EFI driver to RSTe PreOS v5.4.0.1039.
4. Added support for UEFI mode PXE boot of F12 hot key Net boot.
5. Added BIOS/ME downgrade check for SPS 4.0.4.340.
6. Added one event log to record that the event log is full.
7. Displayed PPR setup item.
8. Added support for SATA FLR.
9. Fixed problem of SUM GetSataInfo showing incorrect "Configuration Type" when setting "Configure sSATA as" to "AHCI" or "RAID" on sSATA controller.

10. Fixed problem of Ctrl + Alt + Del causing system to hang after flashing BIOS.
11. Fixed problem of system hanging when installing Linux OS after COM1 & COM2 IO/IRQ exchange.
12. Fixed failure of WDT function.
13. Added workaround for low GPU P2P bandwidth.

2.0b (4/18/2018)
1. Updated CPU microcode to address 'Spectre' variant 2 (CVE 2017-5715) security issue.
2. Enabled IERR crash dump function.
3. Added setup item "SmcBusMasterEn" for enabling Parent bridge of the devices in the gSmcPciForceEnableBusMasterList.
4. Updated 5.12_PurleyCrb_0ACFD085Beta for Purley Skylake platform PLR 4, BKC WW02.
5. Displayed setup item "ACS Control" to Enable/Disable PCIe Access Control Services Extended Capability, with Enabled as default.
6. Changed BIOS revision to 2.0b.
7. Added support for M/B 1.10A with 32MB BIOS chip.
8. Implemented SMC OOB TPM Provisioning via IPMI Feature for customized provisioning table.
9. Changed RC default setting to upgrade POST Memory correctable error to uncorrectable error and map out the channel.
10. Fixed problem of yellow marked device appearing in Windows device manager after S3 resumes.
11. Corrected the "Save Changes" setup option string in "Save & Exit" menu.
12. Disabled SNC once NVDIMM is present in system.
13. Fixed problem of system hanging during BIOS flashing if Watch Dog function is enabled.
14. Fixed problem of TPM 2.0 PS NV Index not being write-protected even if customized provisioning table indicates that it must be write-protected when using "SMC OOB TPM Provisioning via IPMI feature".
15. Fixed problem of system rebooting endlessly when equipping dTPM module.
16. Fixed problem of DMI being cleared when running SUM LoadDefaultBiosCfg.
17. Fixed problem of some platforms hanging up at POST code 0xB2 when equipping dTPM module.
18. Fixed inability of BIOS to boot into OS with Intel P3608 PCIe NVMe drive installed.
19. Disabled CPU2 IIO PCIe root port ACPI hot plug function.
20. Fixed issue with IPMI force boot.
21. Fixed issue of all commands requesting to be persistent.
22. Fixed malfunction of "SMBIOS Preservation" Disabled.
23. Fixed problem of SMC skipping first boot option in UEFI mode when retrying boot.
24. Fixed problem of the endpoint PCIe device having error bits in PCI Status or Device Status register.
25. Fixed inability to set memory policy.
26. Fixed inability to reset the system under DOS by pressing "Ctrl-Alt-Del" on USB keyboard when "Port 60/64 Emulation" is disabled.
27. Fixed failure of BIOS ECO ATT test case 306.
28. Fixed inability of some CPUs to display correct microcode revision under BIOS setup menu.
29. Fixed failure of SATA HSIO register setting test.