BIOS Release Notes Form

Product Name	**X11DPU**
Release Version	**3.8a**
Release Date	**11/15/2022**
Build Date	**10/28/2022**
Previous Version	**3.8**
Update Category	**Critical**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1.[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) (2) For INTEL-TA-00688 Security Advisory to address CVE-2022-26006 (8.2 High), CVE-2022-21198(7.9 High)** **2.[Enhancements] Update token RC_VERSION_VALUE setting to 623.D09.** **3.[Enhancements] Update Intel DCPM UEFI driver to 1.0.0.3536.**
New features	**None**
Fixes	**1.[Fixes] Fix OA2 key injection issue.**

Release Notes from Previous Release(s)

3.8(08/19/2022)

1.[Enhancements] Update AMI label 5.14_PurleyCrb_0ACLA056 for RC0622.D07 2022.2 IPU.
2.[Enhancements] Updated Skylake-SP/Cascade Lake-SP CPU PC microcode for IPU 2022.1.
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] Modify the allocated buffer from EfiBootServicesData to EfiRuntimeServicesData.
8.[Enhancements] Disable MROM1 device since product doesn't use Intel IE function.
9.[Enhancements] Update DBX file to fix Secure Boot Bypass issue.
10.[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)

3.7(06/15/2022)

1 [Enhancements] Change BIOS revision to 3.7.
2 [Enhancements] Update VROC SATA/sSATA legacy driver to VROC PreOS v6.3.5.1003 Hot Fix to fix 10TB or higher volume
drive issue.
3 [Enhancements] Update AEP uEFI driver to 01.00.00.3534 for IPU2022.2.
4 [Enhancements] Update AMI label 5.14_PurleyCrb_0ACLA055 for RC0618.D03 2022.1 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.
5 [Enhancements] Updated Skylake-SP/Cascade Lake-SP CPU PC microcode for IPU 2022.1. (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.
6 [Enhancements] Update BIOS ACM 1.7.54, SINIT ACM 1.7.55 PW for IPU2022.1 to address

7 [Enhancements] Updated Intel Server Platform Services for Purley Refresh Server Platforms IPU2022.1 4.1.4.700

3.6(01/10/2022)

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.

3.5a(08/21/2021)

1.[Enhancements] Update SATA/sSATA EFI driver to VROC PreOS v7.6.0.1012.
1.[Fixes] Fix "Configuration Address Source" show "DHCP" in the setup menu.
2.[Fixes] Fix IPMI page disappear when AOC-URN2-i4GXS is on the bord.
3.[Fixes] Fixed system keep rebooting when install 3 AOC-STG-i4S on MB issue.

3.5(05/31/2021)

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(03/19/2021)

1. Enabled system to boot into PXE with DVD installed.
2. Fixed problem of onboard NVMe1 and NVMe2 items disappearing when AOC-URN2-i4GXS is in the system.

3.4(10/30/2020)

1. Updated AMI label 5.14_PurleyCrb_0ACLA052_BETA for RC update and IPU 2020.2 PV to address Intel-TA-00358: CVE-2020-0587 (6.7, Medium), CVE-2020-0591 (6.7, Medium), and CVE-2020-0592 (3, Low); 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); Intel-TA-00391: CVE-2020-8752 (9.4, Critical), CVE-2020-8753 (8.2, Critical), CVE-2020-12297 (8.2, Critical), CVE-2020-8745 (7.3, Critical), CVE-2020-8705 (7.1, Critical), CVE-2020-12303 (7.0, Critical), CVE-2020-8757 (6.3, Medium), CVE-2020-8756 (6.3, Medium), CVE-2020-8760 (6.0, Medium), CVE-2020-8754 (5.3, Medium), CVE-2020-8747 (4.8, Medium), CVE-2020-12356 (4.4, Medium), CVE-2020-8746 (4.3, Medium), and CVE-2020-8749 (4.2, Medium); Intel-SA-00358: CVE-2020-0590 (7.7, High), CVE-2020-0587 (6.7, Medium), CVE-2020-0591 (6.7, Medium), CVE-2020-0593 (4.7, Medium), CVE-2020-0588 (3.8, Low), and CVE-2020-0592 (3.0, Low); Intel-TA-00391: CVE-2020-8744 (7.2, High), CVE-2020-8705 (7.1, High), and CVE-2020-8755 (4.6, Medium); AMI SA50080 and AMI SA50081: CVE-2020-0570 (7.6, High), CVE-2020-0571 (5.5, Medium), and CVE-2020-8675 (7.1, High); AMI SA-50085: CVE-2020-10713 (8.2, High); and AMI SA-50084: CVE-2020-10255 (9, High) security issues.
2. Added force next boot to UEFI Shell via IPMI support.
3. Added function to move all LANs to the top of boot priority when IPMI forces PXE.
4. Fixed problem of EFI version of PassMark MemTest86 hanging when SMCI Redfish Host Interface is not supported in IPMI firmware.

3.3a(07/21/2020)

1. Deleted repeated boot options which have the same description as the new description.
2. Added inband flash status event log to IPMI MEL.
3. Corrected "Station MAC Address" display order when "Configuration Address Source" is set to "Static".
4. Updated Skylake-SP microcode 6906 and Cascade Lake-SP microcode 2F01 for IPU2020.1.
5. Updated SATA/sSATA RAID OPROM/EFI driver to VROC PreOS v6.3.0.1005 PV.
6. Fixed inability of 6240R and some refresh 4 serial CPU frequencies to reach the maximum when enabling MWAIT.
7. Fixed failure of Secure Erase - Password and problem of BIOS returning "EFI_Device_Error" with SED: Seagate ST1000NX0353.
8. Corrected firmware revision in BIOS Setup.
9. Fixed problem of system hanging at 0xB2 with some NVMe devices.

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 word prompt Control" to control "Hard-Drive word Check" for enabling/disabling HDD word 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 (10/16/2019)
1. Updated AMI label 5.14_PurleyCrb_0ACLA049_BETA for BKC WW36 IPU 2019.2 and AMI security update SA50072.
2. Updated SINIT/BIOS ACM from BKC WW36 IPU 2019.2 to address CVE-2019-0151 and CVE-2019-0152.
3. Updated SPS_E5_04.01.04.339.0 from BKC WW36 IPU 2019.2 to address PSIRT-TA-201905-011.
4. Updated Cascade Lake-SP CPU microcode and Skylake-SP microcode.
5. Displayed Setup item "ARI Support".
6. Added setup item to control 16Gb based Single Die Package DIMM tRFC optimization.
7. Disabled ADDDC/SDDC and set PPR as hPPR.
8. Added Enhanced PPR function and set disabled as default.
9. Removed PXE option for "OnBoard LanX Option ROM" when "Boot mode select" is UEFI.
10. Corrected display of the IPMI AUX revision.

3.1a (07/19/2019)
1. Updated Skylake-SP/Cascade Lake-SP CPU microcode.
2. Updated SPS_E5_04.01.04.323 from BKC WW26 2019.
3. Updated Intel BKCWW26 2019 PV PLR2.
4. Enhanced F12 hot key PXE boot feature.
5. Updated Secure Boot Key to fix the error message of PK key.
6. Updated the behavior for the feature that updates SMBIOS Type 1 and 3 with FRU0.
7. Patched inability of system to boot via onboard LAN2 after IPMI forces PXE boot when there is an OS behind LSI-3108 RAID card.
8. Added back erase NVDIMM routine.
9. Removed Intel Virtualization Technology override when set to extreme performance.
10. Fixed problem of two OS (Redhat & Ubuntu) boot devices appearing in boot order.
11. Fixed failure of OPROM control item if CSM is disabled.

3.1 (04/29/2019)
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. 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.

9. Fixed inability to change IPv6 address or IPv6 Router1 IP address.

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 (03/04/2019)

1. Added support for Purley Refresh platform.
2. Added support for Linux built-in utility efibootmgr.
3. Updated valid range of IPMI setup item VLAN ID to 1-4094.
4. Set NVDIMM ADR timeout to 600us.
5. Added driver health warning message.
6. 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.
7. Modified UEFI network description to IPv4/IPv6 to follow Industry Standard.
8. Patched problem of system hanging at 0x94 when plugging in Nvidia Tesla T4 card.

3.0a (12/21/2018)

1. Added support for Purley Refresh platform.
2. Updated SATA RAID OPROM/EFI driver to RSTe PreOS v6.0.0.1024.
3. Set BMC MAC address to UUID for system without onboard LAN1 or with onboard LAN1 disabled.
4. Set PCIe correctable and uncorrectable (non-fatal) error report to disabled by default.
5. Set RFC4122 encoding to only be enabled for build time produced by IPMI 1.29 or newer.
6. Updated CPU microcode SRV_P_262 for Skylake-SP H0/M0/U0 CPUs.
7. Disabled unused SPS ME "CUPS IIO" and "Volumetric Airflow" sensor.
8. Added 2933 to memory POR.
9. Added support for SATA FLR.
10. Added support for Monitor Mwait feature.
11. Disabled "tRWSR Relaxation" by default.
12. Fixed problem of setup item "Quiet Boot" staying enabled after flashing BIOS with "Quiet Boot" disabled.
13. Added workaround for GPU P2P low bandwidth.
14. Fixed malfunction of disabling Watch Dog while flashing BIOS under OS.
15. Corrected standard NVDIMM ADR time.
16. Fixed failure of CPU PBF (Prioritized Base Frequency).

2.1b (10/16/2018)

1. Added SATA FLR support.
2. Added support for Monitor Mwait feature.
3. Updated SPS 4.0.4.393.
4. Updated CPU microcode SRV_P_253 for Skylake-SP H0/M0/U0 stepping CPUs.
5. Updated SATA RAID OPROM/EFI driver to RSTe PreOS v5.5.0.1028.

6. Updated BIOS ACM 1.3.9 and SINIT ACM 1.3.6.
7. Changed Onboard LAN SMBIOS table from type 9 to type 41.
8. Fixed problem of BIOS always retrying boot when Re-Try Boot is Disabled.
9. Fixed malfunction of LEGACY to EFI support.