BIOS Release Notes Form

Product Name	**X11SPH-NCT(P)F**
Release Version	**4.0**
Release Date	**6/20/2023**
Build Date	**6/20/2023**
Previous Version	**3.9**
Update Category	**Recommended**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Change BIOS revision to 4.0.** **2. Updated AMI label 5.14_PurleyCrb_0ACLA060 for RC0628.P50 IPU 2023.3 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; and for INTEL-SA-00828 Security Advisory to address CVE-2022-40982 (6.5, Medium) security issue.** **3. Updated OEM FID table. Updated token RC_VERSION_VALUE setting to 628.P50. Updated token PRICESSO_0_UCODE_VERSION setting to 02007006. Updated token PRICESSO_2_UCODE_VERSION setting to 04003604. Updated token PRICESSO_3_UCODE_VERSION setting to**

	05003604. Updated token FW_SPS_VERSION setting to 4.1.5.2. **4. Updated Cascade Lake-SP CPU PV microcode for IPU 2023.3.** **5. Updated Intel Server Platform Services for Purley Refresh Server Platforms IPU2023.3 4.1.5.2.** **6. Updated DBX file for AMI-SA50182 SecureBoot DBX Update.**
New features	**N/A**
Fixes	**None**

Release Notes from Previous Release(s)

***3.9 (*3/15/2023)**

1. *Changed BIOS revision to 3.9.*
2. *Updated AMI label 5.14_PurleyCrb_0ACLA059 for RC0627.P11 IPU 2023.2 for INTEL-SA-00807 Security Advisory to address CVE-2022-38087(4.1, Medium) and CVE-2022-33894(7.5, High) security issues; and for INTEL-SA-00717 Security Advisory to address CVE-2022-32231 (7.5, High) / CVE-2022-26343 (8.2, High) security issues.*
3. *Updated token RC_VERSION_VALUE setting to 627.P11. Updated token PRICESSO_0_UCODE_VERSION setting to 02006F05. Updated token PRICESSO_1_UCODE_VERSION setting to 03000012. Updated token PRICESSO_2_UCODE_VERSION setting to 04003501. Updated token PRICESSO_3_UCODE_VERSION setting to 05003501.*
4. *Updated Cascade Lake-SP CPU PV microcode for IPU 2023.2.*

3.8a (10/28/2022)

1. *Updated the AMI label 5.14_PurleyCrb_0ACLA057 for RC0623.D09 2022.3 IPU.*
2. *Updated the token RC_VERSION_VALUE setting to 623.D09, updated the token PRICESSO_0_UCODE_VERSION setting to 02006E05, and updated the token FW_SPS_VERSION setting to 4.1.4.804.*
3. *Updated the Intel DCPM UEFI driver to 1.0.0.3536.*

4. *Updated the Skylake-SP/Cascade Lake-SP CPU PC microcode for IPU 2022.2.*
5. *Fixed the wrong DIMM location display in the event log page.*
6. *Modified the String naming from SMCI to Supermicro.*
7. *Removed "Vendor Keys" in the security page.*
8. *Refined the SMM buffer validation in SmmSmbiosELogInitFuncs.c. Allocated the runtime buffer to trigger ELog SMI in DxeSmmRedirFuncs.c.*
9. *Updated the 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. *Updated the VROC SATA/sSATA legacy driver to VROC PreOS v6.3.5.1003 Hot Fix to fix the 10TB or higher volume drive issue.*
11. *Updated the VROC SATA/sSATA EFI driver to VROC PreOS v7.8.0.1012 to address data loss exposure due to RAID 5 TRIM Support and 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. *Modified the allocated buffer from EfiBootServicesData to EfiRuntimeServicesData.*
13. *Disabled the MROM1 device since it doesn't use the Intel IE function.*
14. *Updated the DBX file to fix the Secure Boot Bypass issue.*
15. *Fixed the OA2 key injection issue.*
16. *Updated the DBX file to fix the Secure Boot Bypass issue.*

3.6 (1/3/2022)

1. *Changed BIOS revision to 3.6.*
2. *Updated SATA/sSATA EFI driver to VROC PreOS v7.7.0.1054.*
3. *Updated AEP uEFI driver to 1.0.0.3531 for IPU2021.2.*
4. *Updated AMI label 5.14_PurleyCrb_0ACLA054 for RC0616.D08 2021.2 IPU for INTEL-SA-00527 Security Advisory to address CVE-021-0103 (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-2021-119 (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. *Updated Intel Server Platform Services for Purley Refresh Server Platforms IPU2021.2 HF1 4.1.4.654.*
6. *Updated 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. *Updated Skylake-SP/Cascade Lake-SP CPU PV microcode for INTEL-SA-00532 Security Advisory to address CVE-2021-0127 (5.6, Medium) security issue and for INTEL-SA-00365 Security Advisory to address CVE-2020-8673 (4.7, Medium) security issue.*

3.5 (6/1/2021)

1. *Updated 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-202012358(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. *Updated 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. *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. *Updated Intel Server Platform Services for Purley Refresh Server Platforms 4.1.4.505.*
5. *Updated AEP FW to FW_1.2.0.5446, uEFI driver to 3515 for IPU2021.1.*
6. *Synchronized IPv6 status in the BIOS and the BMC web.*
7. *Fixed malfunction of the temperature sensor when AOC-STGF-I2S is installed on PCIe slot5.*

3.4a (2/4/2021)

1. *Changed BIOS version to 3.4a.*
2. *Updated Skylake-SP/Cascade Lake-SP CPU PV microcode from Intel-Generic-Microcode-20210125_NDA.*
3. *Updated Intel Server Platform Services for Purley Refresh Server Platforms HF 4 PLR 4.1.4.450.*
4. *Updated SATA/sSATA EFI driver to VROC PreOS v7.5.0.1150.*
5. *Fixed malfunction of the temperature sensor when AOC-STGF-I2S is installed on PCIe slot5.*

3.4 (11/3/2020)

1. *Changed BIOS version to 3.4.*
2. *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).*
3. *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), and CVE-2020-0592 (3, Low) security issues, 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.*
4. *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.*
5. *Updated BIOS ACM 1.7.41 and SINIT ACM 1.7.49 PW for IPU2020.2 to address Intel-TA-00358: CVE-2020-0588 (3.8, Low) and CVE-2020-0590. (7.7, High) security issues.*
6. *Updated SATA/sSATA RAID OPROM/EFI driver to VROC PreOS v6.3.0.1005 PV.*
7. *Updated AEP firmware to FW_1.2.0.5444 to match IPU2020.2.*
8. *Added force next boot to UEFI Shell via IPMI support.*
9. *Added function to move all LANs to the top of boot priority when IPMI forces PXE.*
10. *Added inband flash status event log to IPMI MEL.*
11. *Fixed inability of 6240R and some refresh 4 serial CPU frequencies to reach maximum when enabling Mwait.*
12. *Fixed failure of Secure Erase - Password and problem of BIOS returning "EFI_Device_Error" with SED: Seagate ST1000NX0353.*
13. *Corrected BMC firmware revision in BIOS Setup.*
14. *Fixed problem of system hanging at 0xB2 with some NVMe devices.*
15. *Fixed inconsistency of X-AMI ID of Setup Item "Refresh Watermarks."*

3.3 (2/21/2020)

1. *Changed BIOS version to 3.3.*
2. *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).*
3. *Updated AMI label 5.14_PurleyCrb_0ACLA050 beta for IPU2020.1 PV.*
4. *Updated SPS_E5_04.01.04.381 from IPU 2020.1 PV.*
5. *Updated BIOS ACM 1.7.40 and SINIT ACM 1.7.48 PW.*
6. *Patched problem of system hanging at 94 with new NVidia RTX 6000/8000.*
7. *Enabled saving memory CE location into PPR variable at runtime even if memory correctable error reporting is disabled.*
8. *Added setup item "HDD password prompt Control" to control "Hard-Drive Password Check" for enabling/disabling HDD password prompt window during POST.*
9. *Added SMC HDD Security feature.*
10. *Added support for SMCI USB Remote Network Driver Interface and SMCI USB Universal Network Device Interface, and for Redfish module to get Processor, Memory, and PCIe information.*
11. *Fixed issue of system resetting under ATTO Fiber network card user menu during BIOS POST.*
12. *Fixed mismatch of Secure Boot Mode value.*
13. *Removed requirement to use Admin password for erasing TCG device.*
14. *Fixed problem of two CentOS boot items occurring in boot order if CentOS is installed in RAID 1 system.*

3.2 (12/2/2019)

1. *Changed BIOS version to 3.2.*
2. *Updated AMI label 5.14_PurleyCrb_0ACLA049_BETA for BKC WW36 IPU 2019.2 and AMI security update SA50072.*
3. *Updated SINIT/BIOS ACM from BKC WW36 IPU 2019.2 to address CVE-2019-0151 and CVE-2019-0152.*
4. *Updated SPS_E5_04.01.04.339.0 from BKC WW36 IPU 2019.2 to address PSIRT-TA-201905-011.*
5. *Updated Cascade Lake-SP CPU microcode and Skylake-SP microcode.*
6. *Updated Cascade Lake-SP A0 stepping CPU microcode.*
7. *Updated SATA/sSATA RAID OPROM/EFI driver to VROC PreOS v6.2.0.1034 PC.*
8. *Displayed Setup item "ARI Support".*
9. *Added setup item to control 16Gb based Single Die Package DIMM tRFC optimization.*
10. *Updated Secure Boot Key to fix the error message of PK key.*
11. *Added back erase NVDIMM routine.*
12. *Updated VBIOS and VGA EFI Driver to 1.10.*
13. *Enhanced F12 hot key PXE boot feature.*
14. *Updated the behavior for the feature that updates SMBIOS Type 1 and 3 with FRU0.*
15. *Added a mechanism to show warning message and shut down system if a CPU TDP over specifications is installed.*
16. *Added Redfish/SUM Secure Boot feature to update OOB for secure boot and reserve Key.*
17. *Disabled ADDDC/SDDC and set PPR as hPPR.*
18. *Added sighting CLX28 workaround and downgraded patrol scrub UC to CE.*
19. *Added Enhanced PPR function and set disabled as default.*
20. *Removed PXE option for "OnBoard LanX Option ROM" when "Boot mode select" is UEFI.*
21. *Corrected display of the IPMI AUX revision.*
22. *Changed OOB download and Upload Bios Configuration sequence.*
23. *Fixed problem of two OS (Redhat & Ubuntu) boot devices appearing in boot order.*
24. *Fixed failure of OPROM control item if CSM is disabled.*

25. *Fixed problem of key details showing "Security Violation" after loading Factory secure boot keys.*

3.1 (5/21/2019)

1. *Changed BIOS version to 3.1.*
2. *Updated Skylake-SP/Cascade Lake-SP CPU microcode.*
3. *Updated Intel BKCWW16 2019 PV PLR1.*
4. *Updated SPS_E5_04.01.04.296.0 from BKC WW16 2019.*
5. *Updated SATA/sSATA RAID OPROM/EFI driver to VROC PreOS v6.1.0.1017.*
6. *Update EIP467272 for AMI SA50069, SA50070.*
7. *Set SDDC Plus One or SDDC to disabled by default.*
8. *Set Leaky Bucket that can decrease one memory correctable error count within 2.15 minutes with threshold 512.*
9. *Enhanced BIOS setup menu to auto-switch the Option ROM's value and hide the unexpected value when boot mode changes.*
10. *Updated to SPS 4.0.04.381 or above for INTEL-SA-00213 Security Advisory.*
11. *Set ADDDC Sparing to enable by default.*
12. *Fixed inability to change IPv6 address or IPv6 Router1 IP address.*
13. *Temporarily fixed error for SKX (CLX) 4114 CPU memory training with Micron (18ASF2G72PDZ-2G6E1) RDIMM.*
14. *Fixed failure to boot into VMare OS when set to Maximum Performance, even if Monitor/MWAIT is enabled.*

3.0b (3/04/2019)

1. *Changed BIOS version to 3.0b.*
2. *Added support for Purley Refresh platform.*
3. *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.*
4. *Updated CPU microcode MB750654_0200005A for Skylake-SP H0/M0/U0 stepping CPUs.*
5. *Updated SATA RAID OPROM/EFI driver to RSTe PreOS v6.0.0.1024.*
6. *Added support for Monitor Mwait feature.*
7. *Fixed inability of VMD status to load default if loading default by AFU.*
8. *Added support for SMC HttpBoot.*
9. *Added support for RFC4122 UUID format feature to set RFC4122 encoding from build time produced by IPMICFG 1.29 tool or newer.*
10. *Set PCIe correctable and uncorrectable (non-fatal) error report to disabled by default.*
11. *Disabled unused SPS ME "CUPS IIO" and "Volumetric Airflow" sensor.*
12. *Set NVDIMM ADR timeout to 600us.*
13. *Enhanced the solution for the error/warning message from dmidecode after a modification by AMIDE.*
14. *Prevented inability to update BIOS when CMOS 51 value is 0x0a or 0x1a.*
15. *Fixed problem of BIOS always retrying boot when Re-Try Boot is Disabled.*
16. *Fixed malfunction of support for LEGACY to EFI.*
17. *Fixed failure of Always Turbo in Linux kernel 7.x.*
18. *Fixed malfunction of CPU PBF (Prioritized Base Frequency).*
19. *Fixed incorrect PBF high frequency core number when Hyper-Threading is disabled.*
20. *Modified UEFI network description to IPv4/IPv6 to follow Industry Standard.*

2.1 (8/29/2018)

1. *Updated CPU microcode to address 'Spectre' derivatives (CVE-2018-3639 & CVE-2018-3640) security issue.*
2. *Changed BIOS version to 2.1.*
3. *Updated 5.12_PurleyCrb_0ACFD088 for Purley Skylake platform PLR7, BKC 2018 WW20.*
4. *Updated BIOS ACM 1.3.7 and SINIT ACM 1.3.4.*
5. *Added one event log to record that the event log is full.*
6. *Added support for VMD settings to be preserved after flashing.*
7. *Updated SATA RAID OPROM/EFI driver to RSTe PreOS v5.4.0.1039.*
8. *Corrected BIOS/ME downgrade check for SPS 4.0.4.340.*
9. *Added support for UEFI mode PXE boot of F12 hot key Net boot.*
10. *Added setup item "SmcBusMasterEn" for enabling Parent bridge of the devices in the gSmcPciForceEnableBusMasterList.*
11. *Added support for SATA FLR with enabled as default.*
12. *Fixed problem of DMI being cleared when running SUM UpdateBios.*
13. *Fixed problem of Ctrl + Alt + Del causing system to hang after flashing BIOS.*
14. *Rolled back SVN_3413 to fix failure of WDT function.*
15. *Fixed problem of BIOS reporting incorrect SMBIOS Type 40 when device is installed on Slot 5 and no device is installed on Slot 6.*
16. *Fixed issue with IPMI firmware capability.*

2.0b (2/26/2018)

1. *Updated CPU microcode to address 'Spectre' variant 2 (CVE 2017-5715) security issue.*
2. *Changed BIOS revision to 2.0b.*
3. *Displayed setup item "ACS Control" to Enable/Disable PCIe Access Control Services Extended Capability, with Enabled as default.*
4. *Updated 5.12_PurleyCrb_0ACFD085Beta for Purley Skylake platform PLR 4, BKC WW02.*
5. *Added setup item "SmcBusMasterEn" for enabling Parent bridge of the devices in the gSmcPciForceEnableBusMasterList.*
6. *Fixed failure of BIOS ECO ATT test case 306.*
7. *Fixed inability to reset the system under DOS by pressing "Ctrl-Alt-Del" on USB keyboard when "Port 60/64 Emulation" is disabled.*
8. *Fixed problem of SMC skipping first boot option in UEFI mode when retrying boot.*
9. *Disabled CPU2 IIO PCIe root port ACPI hot plug function.*
10. *Fixed issue with IPMI force boot.*
11. *Fixed inability of some CPUs to display correct microcode revision under BIOS setup menu.*