BIOS Release Notes Form

Product Name	**X11SPM-F/T(P)F**
Release Version	**3.8a SPS 4.1.04.804**
Release Date	**10/28/2022**
Build Date	**10/28/2022**
Previous Version	**3.6**
Update Category	**Recommended**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Updated AMI label 5.14_PurleyCrb_0ACLA057 for RC0623.D09 2022.3 IPU.** **2. Updated token RC_VERSION_VALUE setting to 623.D09. Updated token PRICESSO_0_UCODE_VERSION setting to 02006E05. Updated token FW_SPS_VERSION setting to 4.1.4.804.** **3. Updated Intel DCPM UEFI driver to 1.0.0.3536.** **4. Updated Skylake-SP/Cascade Lake-SP CPU PC microcode for IPU 2022.2 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; 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; and for INTEL-SA-00616 Security Advisory to address CVE-2021-21131(3.3, Low) and CVE-2021-21136(2.7, Low) security issues. **5. Fixed wrong DIMM location in event log page.** **6. Modified String naming from SMCI to Supermicro.** **7. Removed "Vendor Keys" in security page.** **8. Fixed Superdiag hang up issue due to event log abnormal.** **9. Updated 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 VROC SATA/sSATA legacy driver to VROC PreOS v6.3.5.1003 Hot Fix to fix 10TB or higher volume drive issue.** **11. Updated 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 for CVE-2022-29919(7.8 High), CVE-2022-30338(6.7 Medium), CVE-2022-29508(6.3 Medium), and CVE-2022-25976(5.5 Medium).** **12. Disabled MROM1 device.** **13. Updated DBX file to fix Secure Boot Bypass issue.**
New features	**N/A**
Fixes	**1. Fixed OA2 key injection issue.** **2. Enabled IScsi_SUPPORT on Purley generation.** **3. Modified the allocated buffer from EfiBootServicesData to EfiRuntimeServicesData.**

Release Notes from Previous Release(s)

3.6 (1/4/2022)

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 (5/20/2021)

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-2020-2358(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. Added support for IPMI UEFI PXE boot to all LAN ports.
6. Updated SATA/sSATA EFI driver to VROC PreOS v7.5.0.1152.
7. Enabled system to boot into PXE with DVD installed.
8. Added support for IPv6 HTTP Boot function.
9. Fixed a typo in the "PCIe PLL SSC" setup item help string.
10. Removed Intel LAN memory 4G limit when the boot mode is not Legacy.
11. Updated AEP FW to FW_1.2.0.5446 and updated UEFI driver to 3515 for IPU2021.1.
12. Synchronized IPv6 status in the BIOS and the BMC web.
13. Fixed "Configuration Address Source" showing "DHCP" in IPMI IPv6 page.
14. Fixed UEFI OS boot option name showing up incorrectly in BIOS setup.

3.4 (2/20/2021)

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_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.
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 system to boot into PXE with DVD installed.
12. Fixed inability of 6240R and some refresh 4 serial CPU frequencies to reach maximum when enabling Mwait.
13. Fixed failure of Secure Erase - Password and problem of BIOS returning "EFI_Device_Error" with SED: Seagate ST1000NX0353.
14. Corrected BMC firmware revision in BIOS Setup.
15. Fixed problem of system hanging at 0xB2 with some NVMe devices.

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, CVE2020-0549 6.5 Medium), Intel-SA-00288 (CVE2019-11157 5.3 Medium), Intel-SA-00317 (CVE2019-14607 7.9 High).
3. Update 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 to 1.7.40 and SINIT ACM to 1.7.48 PW.
6. Fixed system hanging with NVIDIA RTX 6000/8000 when SR-IOV is disabled.
7. Enabled the memory error correction address to be saved into the PPR variable even if memory correctable error reporting is disabled.
8. Changed patrol scrub from uncorrectable to correctable error as a CLX28 workaround.
9. Added BIOS item "HDD word prompt" to enable/disable HDD word prompt window during POST.
10. Added BIOS support for HDD password erase and reset.

11. Added Redfish functions support.
12. Fixed system automatically rebooting during BIOS POST when ATTO Fiber network card is installed.
13. Fixed the Secure Boot Mode's selected and default option to show "Audit" when the system is in Audit Mode.
14. Removed requirement to use Admin password for erasing TCG device.
15. 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. Changed BIOS version to 3.2.
2. Updated Cascade Lake-SP CPU microcode and Skylake-SP microcode.
3. Updated Cascade Lake-SP A0 stepping CPU microcode.
4. Updated AMI label 5.14_PurleyCrb_0ACLA049_BETA for BKC WW36 IPU 2019.2 and AMI security update SA50072.
5. Updated SPS_E5_04.01.04.339.0 from BKC WW36 IPU 2019.2 to address PSIRT-TA-201905-011.
6. Updated SINIT/BIOS ACM from BKC WW36 IPU 2019.2 to address CVE-2019-0151 and CVE-2019-0152.
7. Updated SATA/sSATA RAID OPROM/EFI driver to VROC PreOS v6.2.0.1034PC.
8. Enhanced F12 hot key PXE boot feature.
9. Added a mechanism to show warning message and shutdown system if a CPU TDP over specifications is installed.
10. Updated the behavior for the feature that updates SMBIOS Type 1 and 3 with FRU0.
11. Added Redfish/SUM Secure Boot feature to update OOB for secure boot and reserve Key.
12. Displayed Setup item "ARI Support".
13. Added setup item to control 16Gb based Single Die Package DIMM tRFC optimization.
14. Added back erase NVDIMM routine.
15. Updated VBIOS and VGA EFI Driver to 1.10.
16. DisabledADDDC/SDDC and set PPR as hPPR.
17. AddedEnhanced PPR functionandset disabled as default.
18. Fixedproblem ofkeydetailsshowing"Security Violation"after loadingFactory secure boot keys.
19. Fixed problem of two OS(Redhat &Ubuntu) boot devicesappearingin boot order.
20. Fixed failure ofOPROM control item if CSM is disabled.
21. Corrected display of the IPMI AUX revision.
22. RemovedPXE option for "OnBoard LanX Option ROM" when "Boot mode select" is UEFI.
23. ChangedOOB download and Upload Bios Configuration sequence.

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. Updated EIP467272 for AMI SA50069, SA50070.
7. Set SDDC Plus One or SDDC to disabled by default.
8. Set ADDDC to enabled by default.
9. Fixed inability to change IPv6 address or IPv6 Router1 IP address.

3.0c (3/27/2019)

1. Updated SPS_E5_04.01.04.296.0 from BKC WW16 2019.
1. Changed BIOS version to 3.0c.
2. Updated CPU microcode version to MB50656_04000021 for Cascade Lake-SP B0 CPUs.
3. Updated CPU microcode version to MB50657_05000021 for Cascade Lake-SP B1 CPUs.
4. Updated AMI label 5.14_PurleyCrb_0ACLA044_BETA for BKC WW10 2019.
5. Updated to SPS 4.0.04.381 or above for INTEL-SA-00213 Security Advisory.
6. Added temporary fix for SKX (CLX) 4114 CPU Memory Training Error with Micron (18ASF2G72PDZ-2G6E1) RDIMM.
7. Fixed failure to boot into VMare OS when set to Maximum Performance, even if Monitor/MWAIT is enabled.
8. Fixed incorrect Bus Number and Device/Function Number of the SMBIOS Type 41 for onboard LANs.
9. Fixed inability of BMC to access chassis information.

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.
21. Fixed issue of no AOC_SAS Temp when AOC-S3108L-H8iR is installed.

2.1 (6/15/2018)

1. Updated CPU microcode to address 'Spectre' derivatives (CVE-2018-3639 & CVE-2018-3640) security issue.
2. Changed BIOS revision 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.
12. Fixed problem ofDMI being cleared when running SUM UpdateBios.
13. Fixed problem of Ctrl + Alt + Del causing system to hang after flashing BIOS.

2.0b (2/26/2018)

1. Updated CPU microcode to address 'Spectre' variant 2 (CVE 2017-5715) security issue.
2. Updated BIOS version to 2.0b.
3. Updated 5.12_PurleyCrb_0ACFD085Beta for Purley Skylake platform PLR 4, BKC WW02.
4. Displayed setup item "ACS Control" to Enable/Disable PCIe Access Control Services Extended Capability, with Enabled as default.
5. Disabled CPU2 IIO PCIe root port ACPI hot plug function.
6. Fixed issue with IPMI force boot.
7. Fixed malfunction of "SMBIOS Preservation" Disabled.
8. Fixed problem of SMC skipping first boot option in UEFI mode when retrying boot.
9. Fixed inability to reset the system under DOS by pressing "Ctrl-Alt-Del" on USB keyboard when "Port 60/64 Emulation" is disabled.
10. Fixed inability of some CPUs to display correct microcode revision under BIOS setup menu.
11. Fixed inability to detect 2 NVMes with AOC 2E2T.
12. Fixed failure of SUM TC 219.