BIOS Release Notes Form

Product Name	**X11SPL-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. Changed BIOS revision to 4.0.** **2. Update 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.** **• For INTEL-SA-00828 Security Advisory to address CVE-2022-40982(6.5, Medium) security issue.** **3. 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 Secure Boot DBX Update.**
New features	**N/A**
Fixes	**N/A**

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 AMI label 5.14_PurleyCrb_0ACLA057 for RC0623.D09 2022.3 IPU.*
2. *Updated token RC_VERSION_VALUE setting to 623.D09.*
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.*
5. *Fixed incorrect DIMM location in the event log page.*
6. *Changed the string from SMC to Supermicro.*

7. *Removed "Vendor Keys" from the security page.*
8. *Updated the following:*
    a. *Refine SMM buffer validation in SmmSmbiosELogInitFuncs*
    b. *Allocate runtime buffer to trigger ELog SMI in DxeSmmRedirFuncs.c*
9. *Updated BIOS ACM 1.7.54, SINIT ACM 1.7.55 PW for IPU2022.1.*
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 Pero's v7.8.0.1012 to address.*
12. *Modified the allocated buffer from EfiBootServicesData to EfiRuntimeServicesData.*
13. *Disabled MROM1 device since product does not use Intel IE function.*
14. *Updated the DBX file to fix the Secure Boot Bypass issue.*
15. *Fixed the OA2 key injection issue.*
16. *Enabled IScsi_SUPPORT.*

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 (5/19/2021)

1. *Updated 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. *Updated BIOS ACM 1.7.43 and 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 feature.*
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. *Corrected typo in "PCIe PLL SSC" setup item help string.*
10. *Removed 4G limit of Intel LAN memory if boot mode is not legacy.*
11. *Updated AEP firmware to FW_1.2.0.5446 and UEFI driver to 3515 for IPU2021.1.*
12. *Synced IPv6 status detection rule with BMC to make sure IPv6 status is the same in BIOS and BMC web.*
13. *Fixed problem of "Configuration Address Source" always showing "DHCP" on IPMI IPv6 page.*
14. *Corrected display of UEFI OS boot option name in BIOS setup.*

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), 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.*
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.*

3.3 (02/21/2020)

1. *Updated AMI label 5.14_PurleyCrb_0ACLA050 beta for IPU2020.1 PV.*
2. *Updated SPS_E5_04.01.04.381 from IPU 2020.1 PV.*
3. *Updated BIOS ACM to 1.7.40 and SINIT ACM to 1.7.48 PW.*
4. *Fixed system hanging with NVIDIA RTX 6000/8000 when SR-IOV is disabled.*
5. *Enabled the memory error correction address to be saved into the PPR variable even if memory correctable error reporting is disabled.*
6. *Changed patrol scrub from uncorrectable to correctable error as a CLX28 workaround.*

7. *Added BIOS item "HDD word prompt" to enable/disable HDD word prompt window during POST.*
8. *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), and Intel-SA-00317 (CVE2019-14607 7.9 High).*
9. *Added BIOS support for HDD password erase and reset.*
10. *Added Redfish functions support.*
11. *Fixed system automatically rebooting during BIOS POST when ATTO Fiber network card is installed.*
12. *Fixed the Secure Boot Mode's selected and default option to show "Audit" when the system is in Audit Mode.*
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. *Updated AMI label 5.14_PurleyCrb_0ACLA049_BETA for BKC WW36 IPU 2019.2 and AMI security update SA50072.*
1. *2.Updated SINIT/BIOS ACM from BKC WW36 IPU 2019.2 to address CVE-2019-0151 and CVE-2019-0152.*
2. *Updated SPS_E5_04.01.04.339.0 from BKC WW36 IPU 2019.2 to address PSIRT-TA-201905-011.*
3. *Updated Cascade Lake-SP CPU microcode and Skylake-SP microcode.*
4. *Displayed Setup item "ARI Support".*
5. *Added setup item to control 16Gb based Single Die Package DIMM tRFC optimization.*
6. *Updated Secure Boot Key to fix the error message of PK key.*
7. *Added back erase NVDIMM routine.*
8. *Updated VBIOS and VGA EFI Driver to 1.10.*
9. *Enhanced F12 hot key PXE boot feature.*
10. *Updated the behavior for the feature that updates SMBIOS Type 1 and 3 with FRU0.*
11. *Added sighting CLX28 workaround and downgraded patrol scrub UC to CE.*
12. *Added Enhanced PPR function and set disabled as default.*
13. *Removed PXE option for "OnBoard LanX Option ROM" when "Boot mode select" is UEFI.*
14. *Corrected display of the IPMI AUX revision.*
15. *Changed OOB download and Upload Bios Configuration sequence.*
16. *Fixed problem of two OS (Redhat &Ubuntu) boot devices appearing in boot order.*
17. *Fixed failure of OPROM control item if CSM is disabled.*
18. *Fixed problem of Call Trace occurring during Cent6.10 installation while Mwait is set to Disabled and ENERGY_PERF_BISA_CFG mode is set to Maximum Performance in BIOS menu.*

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. *Update EIP467272 for AMI SA50069, SA50070.*
6. *Set SDDC Plus One or SDDC to disabled by default.*
7. *Updated SATA/sSATA RAID OPROM/EFI driver to VROC PreOS v6.1.0.1017.*
8. *Set ADDDC Sparing to enable by default.*

9. *Set Leaky Bucket to decrease one memory correctable error count within 2.15 minutes and threshold 512.*
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 inability to change IPv6 address or IPv6 Router1 IP address.*

3.0b (3/4/2018)

1. *Changed BIOS version to 3.0b.*
2. *Added support for Purley Refresh platform.*
3. *Updated CPU microcode MB750654_0200005A for Skylake-SP H0/M0/U0 CPUs.*
4. *Updated SATA RAID OPROM/EFI driver to RSTe PreOS v6.0.0.1024.*
5. *Added support for Monitor Mwait feature.*
6. *Fixed inability of VMD status to load default if loading default by AFU.*
7. *Added support for SMC HttpBoot.*
8. *Set RFC4122 encoding to only be enabled for build time produced by IPMI 1.29 or newer.*
9. *Set PCIe correctable and uncorrectable (non-fatal) error report to disabled by default.*
10. *Disabled unused SPS ME "CUPS IIO" and "Volumetric Airflow" sensor.*
11. *Set NVDIMM ADR timeout to 600us.*
12. *Enhanced the solution for the error/warning message from dmidecode after a modification by AMIDE.*
13. *Added support for Linux built-in utility efibootmgr.*
14. *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.*
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 new 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 tofollow Industry Standard.*

2.1 (6/14/2018)

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. *Added 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. *Corrected BIOS/ME downgrade check for SPS 4.0.4.340.*
12. *Added support for SATA FLR with enabled as default.*
13. *Fixed problem of DMI being cleared when running SUM UpdateBios.*
14. *Fixed problem of Ctrl + Alt + Del causing system to hang after flashing BIOS.*
15. *Fixed missing SMBIOS Type40 information if LAN 2 is on board.*

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. *Updated 5.12_PurleyCrb_0ACFD085Beta for Purley Skylake platform PLR 4, BKC WW02.*
4. *Fixed inability to reset the system under DOS by pressing "Ctrl-Alt-Del" on USB keyboard when "Port 60/64 Emulation" is disabled.*
5. *Fixed problem of SMC skipping first boot option in UEFI mode when retrying boot.*
6. *Displayed setup item "ACS Control" to Enable/Disable PCIe Access Control Services Extended Capability, with Enabled as default.*
7. *Disabled CPU2 IIO PCIe root port ACPI hot plug function.*
8. *Fixed issue with IPMI force boot.*
9. *Fixed malfunction of "SMBIOS Preservation" Disabled.*
10. *Fixed inability of some CPUs to display correct microcode revision under BIOS setup menu.*

2.0a (12/5/2017)

1. *Changed BIOS revision to 2.0a.*
2. *Updated 5.12_PurleyCrb_0ACFD084_BETA for Purley Skylake platform PLR 3.1.*
3. *Updated CPU microcode SRV_P_217 for Skylake-EP H0/M0/U0 stepping CPUs.*
4. *Updated SPS XML setting for SPS 4.0.4.294.*
5. *Displayed "PCIe PLL SSC" setup item for clock spectrum function.*
6. *Enabled display of EarlyVideo message by onboard video when VGA Priority is set to Offboard.*
7. *Removed the "System Firmware Error (POST ERROR)" error log from BMC and "EFI 01030006" in BIOS event log.*
8. *Updated BMC LAN configuration for saving settings of BIOS setup menu.*
9. *Updated help string for tCCD relax setup option.*
10. *Corrected help string of setup item "Enforce POR".*
11. *Updated new MRC error log definition.*
12. *Allowed runtime memory UCE mapout message to be displayed one time during BIOS POST.*
13. *Masked off PCIe correctable and non-fatal errors.*
14. *Moved Run Sure item to Memory RAS Configuration setup page.*
15. *Updated SATA RAID OPROM/EFI driver to RSTe PreOS v5.3.0.1052.*
16. *Added support for AOC-SLG3-2M2 card.*
17. *Hid memory frequency 2200 and 2600.*
18. *Removed support for Ctrl+home triggering recovery.*
19. *Set display of setup option for always turbo mode function as default.*
20. *Added the "PEI--IPMI Initialization" Post-Help message.*
21. *Added Run Sure setup item.*
22. *Set message "BIOS cannot support downgrade to previous version or ROMID mismatch" to show when trying to downgrade BIOS or flash other model of BIOS.*
23. *Fixed failure of Password Preservation Test due to password not being preserved.*
24. *Fixed problem of "Correctable, Non-Fatal and Fatal" error reporting flags being disabled on "Infiniband controller: Mellanox Technologies MT27700 Family [ConnectX-4]" when "PCI PERR/SERR Support" is enabled.*
25. *Fixed failure of setup item "Install Windows 7 USB support".*
26. *Fixed problem of the string of "Error DIMM information" on screen being corrupted when equipping failed DIMM.*
27. *Fixed problem of system sometimes hanging at post code B2 when running Cburn ONOFF.*

28. *Fixed inability to enter setup menu when pressing "DEL" key if there is no boot device.*
29. *Fixed problem of SUM GetDmiInfo command error “Invalid DMI information from BIOS” occurring.*
30. *Fixed failure of SMBIOS Type 20 to fill Interleave Position and Interleaved Data Depth correctly.*
31. *Corrected Hynix DIMM info as "SK Hynix".*
32. *Fixed SUM Test Case #216.*
33. *Fixed problem of IPMI SEL logging "Memory training failure." and "No memory DIMM detected, install memory DIMMs." twice per reboot.*
34. *Fixed problem of TPM 1.2 PS index not being Write-Protected so that the content of TPM 1.2 PS index still can be modified after TPM 1.2 is nvLocked.*
35. *Corrected the "Save Changes" setup option string in "Save & Exit" menu.*
36. *Fixed problem of system generating abnormal strings under DOS after triggering SERR or PERR error event in PCH slot.*
37. *Fixed problem of system hanging when using AFUWIN/AFULNX to flash BIOS under OS.*
38. *Fixed problem of DMI clearing when running SUM LoadDefaultBiosCfg.*