BIOS Release Notes Form

Product Name	**X11SPW-(C)TF(-001)**
Release Version	**4.2**
Release Date	**12/15/2023**
Build Date	**12/15/2023**
Previous Version	**4.1**
Update Category	**Recommended**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Changed BIOS revision to 4.2.** **2. Updated SA50216_Supplement (LogoFAIL Vulnerability).**
New features	**N/A**
Fixes	**N/A**

Release Notes from Previous Release(s)

4.1 (11/24/2023)

1. *Changed BIOS revision to 4.1.*
2. *Updated AMI label 5.14_PurleyCrb_0ACLA061 for RC0628.P59 IPU 2024.1 for AMI Security Advisories SA50191, SA50193, SA50197, SA50198, and SA50205.*
3. *Updated Cascade Lake-SP CPU PV microcode for IPU 2024.1.*
4. *Added OutBand/InBand OemFID support.*
5. *Fixed how BIOS cannot detect riser card when installing AOC-S25GC-i2S.*
6. *Update secure boot KEK and DB key.*

4.0 (6/15/2023)

1. *Changed 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. *Update DBX file for AMI-SA50182 SecureBoot DBX Update.*

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 (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. *Updated token RC_VERSION_VALUE setting to 627.P11.*
4. *Updated Cascade Lake-SP CPU PV microcode for IPU 2023.2.*

3.8a (10/22/2022)

1. *Updated AMI label 5.14_PurleyCrb_0ACLA057 for RC0623.D09 2022.3 IPU.*
2. *Updated token RC_VERSION_VALUE setting to 623.D09. 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.*
5. *Modified the String naming from SMCI to Supermicro.*
6. *Removed "Vendor Keys" in the security page.*
7. *A. Refined SMM buffer validation in SmmSmbiosELogInitFuncs.c*
   B. Allocated runtime buffer to trigger ELog SMI in DxeSmmRedirFuncs.c
8. *Updated BIOS ACM 1.7.54, SINIT ACM 1.7.55 PW for IPU2022.1 to address.*

9. *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.*
10. *Updated VROC SATA/sSATA EFI driver to VROC PreOS v7.8.0.1012 to address.*
11. *Modified the allocated buffer from EfiBootServicesData to EfiRuntimeServicesData.*
12. *Disabled the MROM1 device since it doesn't use Intel IE function.*
13. *Updated the DBX file to fix the Secure Boot Bypass issue.*
14. *Fixed the OA2 key injection issue.*
15. *Fixed the wrong DIMM location display in the event log page.*
16. *Enabled IScsi_SUPPORT on Purley generation.*

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 (5/18/2021)

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. *Updated AEP firmware to FW_1.2.0.5446 and UEFI driver to 3515 for IPU2021.1.*

6. *Synced IPv6 status detection rule with BMC to make sure IPv6 status is the same in BIOS and BMC web.*

3.4a (3/9/2021)

1. *Added support for IPMI UEFI PXE boot to all LAN port feature.*
2. *Updated SATA/sSATA EFI driver to VROC PreOS v7.5.0.1152.*
3. *Fixed inability of the system to boot into PXE with DVD installed.*
4. *Updated Skylake-SP/Cascade Lake-SP CPU PV microcode from Intel-Generic-Microcode-20210125_NDA.*
5. *Updated Intel Server Platform Services for Purley Refresh Server Platforms HF 4 PLR 4.1.4.450.*
6. *Added support for IPv6 HTTP Boot function.*
7. *Corrected typo in "PCIe PLL SSC" setup item help string.*
8. *Removed 4G limit of Intel LAN memory if boot mode is not legacy.*
9. *Fixed SERR/PERR problems from ASC-29320LPE on PCH slot.*
10. *Fixed "Configuration Address Source" always show "DHCP" in IPMI IPv6 page.*
11. *Fixed failure to use SUM to change DCPMM setup item settings.*
12. *Fixed inability of BIOS to detect riser card when installing AOC-S100G-b2C after rebooting system.*
13. *Corrected display of UEFI OS boot option name in BIOS setup.*

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), 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.*
2. *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.*
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. *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).*
12. *Fixed failure of "UEFI Compliant - Boot from iSCSI peripheral" on UEFI SCT test.*
13. *Fixed problem of system hanging during BIOS flash if Watch Dog function is enabled.*
14. *Fixed inability of 6240R and some refresh 4 serial CPU frequencies to reach maximum when enabling Mwait.*
15. *Corrected BMC firmware revision in BIOS Setup.*
16. *Fixed problem of system hanging at 0xB2 with some NVMe devices.*
17. *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 (2/21/2020)

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 1.7.40 and SINIT ACM 1.7.48 PW.*
4. *Patched problem of system hanging at 94 with new NVidia RTX 6000/8000.*
5. *Enabled saving memory CE location into PPR variable at runtime even if memory correctable error reporting is disabled.*
6. *Added sighting CLX28 workaround and downgraded patrol scrub UC to CE.*
7. *Added setup item "HDD password prompt Control" to control "Hard-Drive Password Check" for enabling/disabling HDD password prompt window during POST.*
8. *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).*
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. *Fixed problem of system sometimes hanging in PCIe device's OPROM at POST code B2.*
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 (10/17/2019)

1. *Updated Skylake-SP/Cascade Lake-SP CPU microcode for INTEL-SA-00271 Security Advisory to address CVE-2019-11139 security issue, and for INTEL-SA-00270 Security Advisory to address CVE-2019-11135 security issue.*
2. *Updated SPS_E5_04.01.04.339.0 from BKC WW36 IPU 2019.2 to address PSIRT-TA-201905-011 for INTEL-SA-00241 Security Advisory to address CVE-2019-11090, CVE-2019-11088, CVE-2019-0165, CVE-2019-0166, CVE-2019-0168, CVE-2019-0169, CVE-2019-11086, CVE-2019-11087, CVE-2019-11101, CVE-2019-11100, CVE-2019-11102, CVE-2019-11103, CVE-2019-11104, CVE-2019-11105, CVE-2019-11106, CVE-2019-11107, CVE-2019-11108, CVE-2019-11110, CVE-2019-11097, CVE-2019-0131, CVE-2019-11109, CVE-2019-11131, CVE-2019-11132, and CVE-2019-11147 security issues.*
3. *Updated AMI label 5.14_PurleyCrb_0ACLA049_BETA for BKC WW36 IPU 2019.2 and AMI security update SA50072 for INTEL-SA-00280 Security Advisory to address CVE-2019-11136 and CVE-2019-11137 security issues.*
4. *Updated BIOS ACM 1.7.3 and SINIT ACM 1.7.45 PW from BKC WW36 IPU 2019.2 for INTEL-SA-00240 Security Advisory to address CVE-2019-0151 and CVE-2019-0152.*
5. *Updated SATA/sSATA RAID OPROM/EFI driver to VROC PreOS v6.2.0.1034.*
6. *Added support for firmware version information.*
7. *Disabled ADDDC/SDDC and set PPR as hPPR.*
8. *Removed PXE option for "OnBoard LanX Option ROM" when "Boot mode select" is UEFI.*
9. *Fixed ability to see memory correctable error event during MRC when use a single bit bad DIMM.*

3.0b (5/22/2019)

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 problem of "?[1;31;40m" showing on POST screen when EFI driver is "Unhealthy".*
10. *Fixed inability to change IPv6 address or IPv6 Router1 IP address.*
11. *Fixed malfunction of workaround for GPU P2P low bandwidth.*

3.0b (3/4/2019)

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_04.01.04.256.0 from Intel BKCWW08.*
5. *Updated SATA RAID OPROM/EFI driver to RSTe PreOS v6.0.0.1024.*
6. *Set PCIe correctable and uncorrectable (non-fatal) error report to disabled by default.*
7. *Added support for RFC4122 UUID format feature to set RFC4122 encoding from build time produced by IPMICFG 1.29 tool or newer.*
8. *Disabled unused SPS ME "CUPS IIO" and "Volumetric Airflow" sensor.*
9. *Added support for Linux built-in utility efibootmgr.*
10. *Updated IPv6 router-related setup item string.*
11. *Reduced redundant reboot for offboard VGA switching.*
12. *Set NVDIMM ADR timeout to 600us.*
13. *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.*
14. *Fixed problem of setup item "Quiet Boot" staying enabled after flashing BIOS with "Quiet Boot" disabled.*
15. *Modified UEFI network description to IPv4/IPv6 to follow Industry Standard.*
16. *Patched problem of system hanging at 0x94 when plugging in Nvidia Tesla T4 card.*
17. *Fixed inability of "Network Stack"-related items to get/change via SUM OOB method.*

2.1a (9/17/2018)

1. *Added support for SATA FLR.*
2. *Added a patch to prevent reboot hang when installing AVAL APX-3224 card.*
3. *Added support for IPV6 address multiline feature on IPMI page.*
4. *Added support for Monitor Mwait feature.*
5. *Updated SPS 4.0.4.381 for INTEL-SA-00131 Security Advisory to address CVE-2018-3643 and CVE-2018-3644 security issues.*
6. *Updated CPU microcode SRV_P_253 for Skylake-SP H0/M0/U0 stepping CPUs.*
7. *Fixed problem of system resetting while flashing BIOS under OS if Watch Dog function is enabled.*

8. *Fixed malfunction of BIOS/ME downgrade check when running flash package (SWJPME2) a second time.*
9. *Fixed problem of BIOS always retrying boot when Re-Try Boot is Disabled.*
10. *Fixed malfunction of support for LEGACY to EFI.*
11. *Fixed issue with IPMI firmware capability.*
12. *Patched missing PSU information if common header is empty.*
13. *Fixed failure of turbo in new Linux kernel.*

2.1 (6/14/2018)

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. *Fixed problem of SUM GetSataInfo showing incorrect "Configuration Type" when setting "Configure sSATA as" to "AHCI" or "RAID" on sSATA controller.*
9. *Fixed problem of Ctrl + Alt + Del causing system to hang after flashing BIOS.*
10. *Fixed problem of system hanging when installing Linux OS after COM1 & COM2 IO/IRQ exchange.*
11. *Fixed failure of WDT function.*

2.0b (2/26/2018)

1. *Updated CPU microcode to address 'Spectre' variant 2 (CVE 2017-5715) security issue.*
2. *Updated 5.12_PurleyCrb_0ACFD085Beta for Purley Skylake platform PLR 4, BKC WW02.*
3. *Enabled IERR crash dump function.*
4. *Added setup item "SmcBusMasterEn" for enabling Parent bridge of the devices in the gSmcPciForceEnableBusMasterList.*
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. *Implemented SMC OOB TPM Provisioning via IPMI Feature for customized provisioning table.*
8. *Changed RC default setting to upgrade POST Memory correctable error to uncorrectable error and map out the channel.*
9. *Changed the disabling of CPU Core by core number.*
10. *Corrected the "Save Changes" setup option string in "Save & Exit" menu.*
11. *Disabled SNC once NVDIMM is present in system.*
12. *Fixed problem of system hanging during BIOS flashing if Watch Dog function is enabled.*
13. *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".*
14. *Fixed problem of DMI being cleared when SUM LoadDefaultBiosCfg is run.*
15. *Fixed inability of BIOS to boot into OS with Intel P3608 PCIe NVMe drive installed.*
16. *Fixed issue with IPMI force boot.*
17. *Fixed issue of all commands requesting to be persistent.*
18. *Fixed malfunction of "SMBIOS Preservation" Disabled.*
19. *Fixed problem of SMC skipping first boot option in UEFI mode when retrying boot.*

20. *Fixed problem of the endpoint PCIe device having error bits in PCI Status or Device Status register.*
21. *Fixed inability to set memory policy.*
22. *Fixed inability to reset the system under DOS by pressing "Ctrl-Alt-Del" on USB keyboard when "Port 60/64 Emulation" is disabled.*
23. *Fixed failure of BIOS ECO ATT test case 306.*
24. *Fixed inability of some CPUs to display correct microcode revision under BIOS setup menu.*