BIOS Release Notes Form

Product Name	**X11SPi-TF**
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. *Update secure boot KEK and DB key.*

***4.0 (*6/20/2023)**

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. *Updated 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 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. *Event log page displayed the incorrect DIMM location.*
6. *String name was changed from SMCI to Supermicro.*
7. *"Vendor Keys" has been removed from the security page.*

8. *a.) Improved SMM buffer validation in SmmSmbiosELogInitFuncs.c.*
   b.) In DxeSmmRedirFuncs.c, a runtime buffer was allocated to trigger ELog SMI.
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… 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)*
12. *Allocated buffer was changed from EfiBootServicesData to EfiRuntimeServicesData.*
13. *Since the product does not use the Intel IE function, the MROM1 device has been disabled.*
14. *Updated DBX file to fix Secure Boot Bypass issue.*
15. *Fixed OA2 key injection issue.*
16. *IScsi SUPPORT has been enabled on the 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 RC 612.D02 and IPU 2021.1 PV 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 (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. *Deleted repeated boot options which have the same description as the new description.*
5. *Added inband flash status event log to IPMI MEL.*
6. *Corrected "Station MAC Address" display order when "Configuration Address Source" is set to "Static".*
7. *Updated SATA/sSATA RAID OPROM/EFI driver to VROC PreOS v6.3.0.1005 PV.*
8. *Fixed problem of EFI version of PassMark MemTest86 hanging when SMCI Redfish Host Interface is not supported in IPMI firmware.*
9. *Fixed inability of 6240R and some refresh 4 serial CPU frequencies to reach maximum when enabling Mwait.*
10. *Fixed failure of Secure Erase - Password and problem of BIOS returning "EFI_Device_Error" with SED: Seagate ST1000NX0353.*
11. *Corrected BMC firmware revision in BIOS Setup.*
12. *Fixed problem of system hanging at 0xB2 with some NVMe devices.*

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. *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 (10/17/2019)

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. *Updated Secure Boot Key to fix the error message of PK key.*
8. *Patched inability of system to boot via onboard LAN2 after IPMI forces PXE boot when there is an OS behind LSI-3108 RAID card.*
9. *Added back erase NVDIMM routine.*
10. *Updated VBIOS and VGA EFI Driver to 1.10.*
11. *Enhanced F12 hot key PXE boot feature.*
12. *Updated the behavior for the feature that updates SMBIOS Type 1 and 3 with FRU0.*
13. *Disabled ADDDC/SDDC and set PPR as hPPR.*
14. *Added Enhanced PPR function and set disabled as default.*
15. *Removed PXE option for "OnBoard LanX Option ROM" when "Boot mode select" is UEFI.*
16. *Corrected display of the IPMI AUX revision.*
17. *Changed OOB download and Upload Bios Configuration sequence.*
18. *Fixed problem of two OS (Redhat & Ubuntu) boot devices appearing in boot order.*
19. *Fixed failure of OPROM control item if CSM is disabled.*

3.0b (3/4/2019)

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. *Added support for RFC4122 UUID format feature to set RFC4122 encoding from build time produced by IPMICFG 1.29 tool or newer.*
6. *Updated CPU microcodes from SRV_P_270.*
7. *Disabled unused SPS ME "CUPS IIO" and "Volumetric Airflow" sensor.*
8. *Added 2933 to memory POR.*
9. *Implemented SMBIOS type 161 for multi-chip ultra riser card.*
10. *Added support for Linux built-in utility efibootmgr.*
11. *Updated valid range of IPMI setup item VLAN ID to 1-4094.*
12. *Added driver health warning message.*
13. *Set NVDIMM ADR timeout to 600us.*
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 setup item "Quiet Boot" staying enabled after flashing BIOS with "Quiet Boot" disabled.*
16. *Fixed incorrect PBF high frequency core number when Hyper-Threading is disabled.*
17. *Added workaround for failure of BIOS flash with 156 bytes PubKey (Error: "Secure Flash Rom Verify Fail").*
18. *Modified UEFI network description to IPv4/IPv6 to follow Industry Standard.*
19. *Patched problem of system hanging at 0x94 when plugging in Nvidia Tesla T4 card.*

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. *Added setup item "SmcBusMasterEn" for enabling Parent bridge of the devices in the gSmcPciForceEnableBusMasterList.*
3. *Updated Purley RC 151.R03.*
4. *Displayed setup item "ACS Control" to Enable/Disable PCIe Access Control Services Extended Capability, with Enabled as default.*
5. *Changed RC default setting to upgrade POST Memory correctable error to uncorrectable error and map out the channel.*

6. *Fixed problem of DMI being cleared when running SUM LoadDefaultBiosCfg.*
7. *Disabled CPU2 IIO PCIe root port ACPI hot plug function.*
8. *Fixed issue with IPMI force boot.*
9. *Fixed problem of SMC skipping first boot option in UEFI mode when retrying boot.*
10. *Fixed inability to reset the system under DOS by pressing "Ctrl-Alt-Del" on USB keyboard when "Port 60/64 Emulation" is disabled.*
11. *Fixed inability of some CPUs to display correct microcode revision under BIOS setup menu.*