IPMI Firmware / BIOS Release Notes Form

Product Name	**X11SPH-NCT(P)F**
Release Version	**3.3**
Release Date	**2/21/2020**
Build Date	**2/21/2020**
Previous Version	**3.2**
Update Category	**Critical**
Dependencies	**None**
Important Notes	**None**
Enhancements	**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.
New features	N/A
Fixes	1. Fixed mismatch of Secure Boot Mode value. 2. Removed requirement to use Admin password for erasing TCG device. 3. 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.