IPMI Firmware / BIOS Release Notes Form

Product Name	**X11SPI-TF**
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. 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.**
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.**

Release Notes from Previous Release(s)

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.