IPMI Firmware / BIOS Release Notes Form

Product Name	**X11SPL-F**
Release Version	**3.1**
Release Date	**5/21/2019**
Previous Version	**3.0b**
Update Category	**Critical**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Changed BIOS version to 3.1.** **2. Updated Skylake-SP/Cascade Lake-SP CPU microcode for for INTEL-SA-00233 Security Advisory.** **3. Updated to SPS 4.0.04.381 or above for INTEL-SA-00213 Security Advisory.** **4. Updated Intel BKCWW16 2019 PV PLR1.** **5. Updated SPS_E5_04.01.04.296.0 from BKC WW16 2019.** **6. Update EIP467272 for AMI SA50069, SA50070.** **7. Set SDDC Plus One or SDDC to disabled by default.** **8. Updated SATA/sSATA RAID OPROM/EFI driver to VROC PreOS v6.1.0.1017.** **9. Set ADDDC Sparing to enable by default.** **10. Set Leakey bucket to decrease one memory correctable error count within 2.15 minutes and threshold 512.**

New features	**N/A**
Fixes	**1. 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.** **2. Fixed inability to change IPv6 address or IPv6 Router1 IP address.**

Release Notes from Previous Release(s)

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 to follow 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.