IPMI Firmware / BIOS Release Notes Form

Product Name	**X11SPG-TF**
Release Version	**2.1**
Release Date	**6/19/2018**
Previous Version	**2.0b**
Update Category	**Critical**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Updated CPU microcode to address 'Spectre' derivatives (CVE-2018-3639 & CVE-2018-3640) security issue.** **2. Fixed inability of AFUWIN to keep VMD setting.** **3. Corrected default setting for Enable SmcBusMasterEn setup item.** **4. Added BIOS/ME downgrade check for SPS 4.0.4.340.** **5. Added hidden item "Early Console Logo".** **6. Added support for RFC3021.** **7. Added support for UEFI mode PXE boot of F12 hot key Net boot.** **8. Changed X11SPG BIOS revision to 2.1.** **9. Updated Purley RC 154.R13, SPS 4.0.04.340 and ACM 1.3.7, SINIT ACM 1.3.4.** **10. Updated SATA RAID OPROM/EFI driver to RSTe PreOS v5.4.0.1039.** **11. Corrected BIOS/ME downgrade check for SPS 4.0.4.340.**

	12. Corrected help message for TPH BIOS setup items. 13. Displayed PPR setup item.
New features	N/A
Fixes	1. Fixed problem of SUM GetSataInfo showing incorrect "Configuration Type" when setting "Configure sSATA as" to "AHCI" or "RAID" on sSATA controller. 2. Fixed problem of DMI being cleared when running SUM UpdateBios. 3. Fixed problem of Ctrl + Alt + Del causing system to hang after flashing BIOS.

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 "Power Technology" callback solution.
4. Updated 5.12_PurleyCrb_0ACFD085Beta for Purley Skylake platform PLR 4, BKC WW02.
5. Displayed setup item "ACS Control" to Enable/Disable PCIe Access Control Services Extended Capability, with Enabled as default.
6. Enabled IERR crash dump function.
7. Changed maximum speed in SMBIOS type 4 to 4500Mhz.
8. Added one event log to record that the event log is full.
9. Added support for VMD settings to be preserved after flashing, with enabled as default.
10. Changed RC default setting to upgrade POST Memory correctable error to uncorrectable error and map out the channel.
11. Implemented SMC OOB TPM Provisioning via IPMI Feature for customized provisioning table.
12. Fixed issue with IPMI force boot.
13. Fixed issue of all commands requesting to be persistent.
14. Fixed problem of incorrect memory access on OOB causing system to hang.
15. Fixed malfunction of "SMBIOS Preservation" Disabled.
16. Fixed problem of SMC skipping first boot option in UEFI mode when retrying boot.
17. Fixed problem of the endpoint PCIe device having error bits in PCI Status or Device Status register.
18. Fixed inability to set memory policy.
19. Fixed inability to reset the system under DOS by pressing "Ctrl-Alt-Del" on USB keyboard when "Port 60/64 Emulation" is disabled.
20. Fixed problem of some platforms hanging up at POST code 0xB2 when equipping dTPM module.
21. Fixed problem of DMI being cleared when running SUM LoadDefaultBiosCfg.
22. 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".
23. Fixed problem of system hanging during BIOS flashing if Watch Dog function is enabled.
24. Corrected the "Save Changes" setup option string in "Save & Exit" menu.
25. Fixed problem of changing CPU Core Enable/Disable in setup menu sometimes not taking effect on Windows OS.
26. Fixed problem of system generating abnormal strings under DOS after triggering SERR or PERR error event in PCH slot.
27. Fixed inability of some CPUs to display correct microcode revision under BIOS setup menu.