IPMI Firmware / BIOS Release Notes Form

Product Name	**X11SPW-(C)TF**
Release Version	**2.1**
Release Date	**6/14/2018**
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. 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.**
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 Ctrl + Alt + Del causing system to hang after flashing BIOS.** **3. Fixed problem of system hanging when installing Linux OS after COM1 & COM2 IO/IRQ exchange.** **4. Fixed failure of WDT function.**

Release Notes from Previous Release(s)

2.0b (2/26/2018)

1. Updated CPU microcode to address 'Spectre' variant 2 (CVE 2017-5715) security issue.
2. Updated 5.12_PurleyCrb_0ACFD085Beta for Purley Skylake platform PLR 4, BKC WW02.
3. Enabled IERR crash dump function.
4. Added setup item "SmcBusMasterEn" for enabling Parent bridge of the devices in the gSmcPciForceEnableBusMasterList.
5. Displayed setup item "ACS Control" to Enable/Disable PCIe Access Control Services Extended Capability, with Enabled as default.
6. Changed BIOS revision to 2.0b.
7. Implemented SMC OOB TPM Provisioning via IPMI Feature for customized provisioning table.
8. Changed RC default setting to upgrade POST Memory correctable error to uncorrectable error and map out the channel.
9. Changed the disabling of CPU Core by core number.
10. Corrected the "Save Changes" setup option string in "Save & Exit" menu.
11. Disabled SNC once NVDIMM is present in system.
12. Fixed problem of system hanging during BIOS flashing if Watch Dog function is enabled.
13. 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".
14. Fixed problem of DMI being cleared when SUM LoadDefaultBiosCfg is run.
15. Fixed inability of BIOS to boot into OS with Intel P3608 PCIe NVMe drive installed.
16. Fixed issue with IPMI force boot.
17. Fixed issue of all commands requesting to be persistent.
18. Fixed malfunction of "SMBIOS Preservation" Disabled.
19. Fixed problem of SMC skipping first boot option in UEFI mode when retrying boot.
20. Fixed problem of the endpoint PCIe device having error bits in PCI Status or Device Status register.
21. Fixed inability to set memory policy.
22. Fixed inability to reset the system under DOS by pressing "Ctrl-Alt-Del" on USB keyboard when "Port 60/64 Emulation" is disabled.
23. Fixed failure of BIOS ECO ATT test case 306.
24. Fixed inability of some CPUs to display correct microcode revision under BIOS setup menu.