IPMI Firmware / BIOS Release Notes Form

Supermicro disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade. All products, computer systems, dates, and figures specified are preliminary based on current expectations, and are subject to change without notice. Supermicro and the Supermicro logo are trademarks of Super Micro Computer, Inc. in the U.S. and/or other countries.

Product Name	**X11SPI-TF**
Release Version	**3.0b**
Release Date	**3/4/2019**
Previous Version	**2.1**
Update Category	**Recommended**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Added support for Purley Refresh platform.** **2. Updated SATA RAID OPROM/EFI driver to RSTe PreOS v6.0.0.1024.** **3. Set PCIe correctable and uncorrectable (non-fatal) error report to disabled by default.** **4. Added support for RFC4122 UUID format feature to set RFC4122 encoding from build time produced by IPMICFG 1.29 tool or newer.** **5. Updated CPU microcodes from SRV_P_270.** **6. Disabled unused SPS ME "CUPS IIO" and "Volumetric Airflow" sensor.** **7. Added 2933 to memory POR.** **8. Added support for Linux built-in utility efibootmgr.** **9. Updated valid range of IPMI setup item VLAN ID to 1-4094.** **10. Added driver health warning message.** **11. Set NVDIMM ADR timeout to 600us.**

	12. 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.
New features	**N/A**
Fixes	**1. Fixed problem of setup item "Quiet Boot" staying enabled after flashing BIOS with "Quiet Boot" disabled.** **2. Fixed incorrect PBF high frequency core number when Hyper-Threading is disabled.** **3. Added workaround for failure of BIOS flash with 156 bytes PubKey (Error: "Secure Flash Rom Verify Fail").** **4. Modified UEFI network description to IPv4/IPv6 to follow Industry Standard.** **5. Patched problem of system hanging at 0x94 when plugging in Nvidia Tesla T4 card.**

Release Notes from Previous Release(s)

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.