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. Copyright © 2018 Super Micro Computer, Inc. All rights reserved.

Product Name	**X11SPG-TF**
Release Version	**3.0b**
Release Date	**3/11/2019**
Previous Version	**3.0a**
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 microcode SRV_P_262 for Skylake-SP H0/M0/U0 stepping CPUs.** **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. Prevented inability to flash BIOS by AFU or SUM inband when JPME2 CMOS value is not accepted.** **13. Added a help/reminder message when a user incorrectly selects “EFI” for “Onboard Video Option Room” to avoid user confusion.** **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.**
New features	**N/A**
Fixes	**1. Fixed problem of setup item "Quiet Boot" staying enabled after flashing BIOS with "Quiet Boot" disabled.** **2. Fixed failure of workaround for BIOS flash with 156 bytes PubKey (Error: “Secure Flash Rom Verify Fail”).** **3. Modified UEFI network description to IPv4/IPv6 to follow Industry Standard.** **4. Patched system from hanging 0x94 when plugging in NVIDIA Tesla T4 card.** **5. Fixed incorrect display of TDP in Intel Speed Select table.** **6. Fixed failure of AOC sensor reading when directly plugging a PCIe card in CPU PCI slot.**

Release Notes from Previous Release(s)

2.1a (9/5/2018)

1. Set PCIe link status to be polled at DXE stage to fix wrong information in BIOS setup IIO page.
2. Changed MAX_ITEM_STRING_SIZE to 128 bytes when updating Help string by SetString.
3. Updated SPS 4.0.4.381 for INTEL-SA-00131 Security Advisory to address CVE-2018-3643 and CVE-2018-3644 security issues.
4. Added support for Monitor Mwait feature.
5. Added support for IPV6 address multiline feature on IPMI page.
6. Updated 5.12_PurleyCrb_0ACFD089Beta security update.
7. Added a patch to prevent reboot hang when installing AVAL APX-3224 card.
8. Added support for SATA FLR.
9. Fixed failure of system downgrade from SPS 4.0.4.381 to 4.0.4.340.
10. Fixed failure of turbo in new Linux kernel.
11. Patched missing PSU information if common header is empty.
12. Fixed issue with IPMI firmware capability for SIOM projects.
13. Fixed malfunction of support for LEGACY to EFI.
14. Fixed problem of BIOS always retrying boot when Re-Try Boot is Disabled.
15. Fixed malfunction of BIOS/ME downgrade check when running flash package (SWJPME2) a second time.
16. Fixed problem of system resetting while flashing BIOS under OS if Watch Dog function is enabled.
17. Added workaround for low GPU P2P bandwidth.
18. Fixed problem of system always rebooting after flashing BIOS that has password preset and quiet boot disabled.

2.1 (6/19/2018)

1. Updated CPU microcode to address ‘Spectre’ derivatives (CVE-2018-3639 & CVE-2018-3640) security issue.
2. Corrected default setting for Enable SmcBusMasterEn setup item.
3. Added BIOS/ME downgrade check for SPS 4.0.4.340.
4. Added hidden item "Early Console Logo".
5. Added support for RFC3021.
6. Added support for UEFI mode PXE boot of F12 hot key Net boot.
7. Changed X11SPG BIOS revision to 2.1.
8. Updated Purley RC 154.R13, SPS 4.0.04.340 and ACM 1.3.7, SINIT ACM 1.3.4.
9. Updated SATA RAID OPROM/EFI driver to RSTe PreOS v5.4.0.1039.
10. Corrected BIOS/ME downgrade check for SPS 4.0.4.340.
11. Corrected help message for TPH BIOS setup items.
12. Displayed PPR setup item.
13. Fixed inability of AFUWIN to keep VMD setting.
14. Fixed problem of SUM GetSataInfo showing incorrect "Configuration Type" when setting "Configure sSATA as" to "AHCI" or "RAID" on sSATA controller.
15. Fixed problem of DMI being cleared when running SUM UpdateBios.
16. Updated 10G LAN EFI driver 6.7.0.4 (IBA 23.1) to address onboard X540 UEFI PXE failure issue.
17. Fixed problem of system hanging when installing Linux OS after COM1 & COM2 IO/IRQ exchange.
18. 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. Added support for VMD settings to be preserved after flashing, with disabled as default.
5. Updated 5.12_PurleyCrb_0ACFD085Beta for Purley Skylake platform PLR 4, BKC WW02.
6. Displayed setup item "ACS Control" to Enable/Disable PCIe Access Control Services Extended Capability, with Enabled as default.
7. Fine tuned maximum payload for NVMe device.
8. Enabled IERR crash dump function.
9. Added MMIO prelocation for JBOF NVMe.
10. Changed maximum speed in SMBIOS type 4 to 4500Mhz.
11. Added one event log to record that the event log is full.
12. Added support for VMD settings to be preserved after flashing, with enabled as default.
13. Changed RC default setting to upgrade POST Memory correctable error to uncorrectable error and map out the channel.
14. Added UIO LAN control function.
15. Implemented SMC OOB TPM Provisioning via IPMI Feature for customized provisioning table.
16. Fixed inability of BIOS to boot into OS with Intel P3608 PCIe NVMe drive installed.
17. Fixed issue with IPMI force boot.
18. Fixed issue of all commands requesting to be persistent.
19. Fixed problem of incorrect memory access on OOB causing system to hang.
20. Fixed malfunction of "SMBIOS Preservation" Disabled.
21. Fixed problem of SMC skipping first boot option in UEFI mode when retrying boot.
22. Fixed problem of the endpoint PCIe device having error bits in PCI Status or Device Status register.
23. Fixed inability to set memory policy.
24. Fixed inability to reset the system under DOS by pressing "Ctrl-Alt-Del" on USB keyboard when "Port 60/64 Emulation" is disabled.
25. Fixed problem of some platforms hanging up at POST code 0xB2 when equipping dTPM module.
26. Fixed problem of DMI being cleared when running SUM LoadDefaultBiosCfg.
27. 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".
28. Fixed problem of system hanging during BIOS flashing if Watch Dog function is enabled.
29. Corrected the "Save Changes" setup option string in "Save & Exit" menu.
30. Disabled SNC once NVDIMM is present in system.
31. Fixed problem of changing CPU Core Enable/Disable in setup menu sometimes not taking effect on Windows OS.
32. Fixed problem of system generating abnormal strings under DOS after triggering SERR or PERR error event in PCH slot.
33. Fixed inability of some CPUs to display correct microcode revision under BIOS setup menu.