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	**X11SPW-(C)TF**
Release Version	**3.0b**
Release Date	**3/4/2019**
Previous Version	**2.1a**
Update Category	**Recommended**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Added support for Purley Refresh platform.** **2. Updated CPU microcodes from SRV_P_270.** **3. Updated SINIT ACM 1.7.2 PW from BKC WW06 2019.** **4. Updated SPS_E5_04.01.04.256.0 from Intel BKCWW08.** **5. Updated SATA RAID OPROM/EFI driver to RSTe PreOS v6.0.0.1024.** **6. Set PCIe correctable and uncorrectable (non-fatal) error report to disabled by default.** **7. Added support for RFC4122 UUID format feature to set RFC4122 encoding from build time produced by IPMICFG 1.29 tool or newer.** **8. Disabled unused SPS ME "CUPS IIO" and "Volumetric Airflow" sensor.** **9. Added support for Linux built-in utility efibootmgr.** **10. Updated IPv6 router-related setup item string.** **11. Reduced redundant reboot for offboard VGA switching.**

	12. Set NVDIMM ADR timeout to 600us. **13. 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. Modified UEFI network description to IPv4/IPv6 to follow Industry Standard.** **3. Patched problem of system hanging at 0x94 when plugging in Nvidia Tesla T4 card.** **4. Fixed inability of "Network Stack"-related items to get/change via SUM OOB method.**

Release Notes from Previous Release(s)

2.1a (9/17/2018)

1. Added support for SATA FLR.
2. Added a patch to prevent reboot hang when installing AVAL APX-3224 card.
3. Added support for IPV6 address multiline feature on IPMI page.
4. Added support for Monitor Mwait feature.
5. Updated SPS 4.0.4.381 for INTEL-SA-00131 Security Advisory to address CVE-2018-3643 and CVE-2018-3644 security issues.
6. Updated CPU microcode SRV_P_253 for Skylake-SP H0/M0/U0 stepping CPUs.
7. Fixed problem of system resetting while flashing BIOS under OS if Watch Dog function is enabled.
8. Fixed malfunction of BIOS/ME downgrade check when running flash package (SWJPME2) a second time.
9. Fixed problem of BIOS always retrying boot when Re-Try Boot is Disabled.
10. Fixed malfunction of support for LEGACY to EFI.
11. Fixed issue with IPMI firmware capability.
12. Patched missing PSU information if common header is empty.
13. Fixed failure of turbo in new Linux kernel.

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. 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.