

# 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.*

<b>Product Name</b>	<b>X11SPM-F/TF/TPF</b>
<b>Release Version</b>	<b>3.0b</b>
<b>Release Date</b>	<b>3/04/2019</b>
<b>Previous Version</b>	<b>2.1</b>
<b>Update Category</b>	<b>Recommended</b>
<b>Dependencies</b>	<b>None</b>
<b>Important Notes</b>	<b>None</b>
<b>Enhancements</b>	<ol style="list-style-type: none"><li>1. Changed BIOS version to 3.0b.</li><li>2. Added support for Purley Refresh platform.</li><li>3. 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.</li><li>4. Updated CPU microcode MB750654_0200005A for Skylake-SP H0/M0/U0 stepping CPUs.</li><li>5. Updated SATA RAID OROM/EFI driver to RSTe PreOS v6.0.0.1024.</li><li>6. Added support for Monitor Mwait feature.</li><li>7. Fixed inability of VMD status to load default if loading default by AFU.</li><li>8. Added support for SMC HttpBoot.</li><li>9. Added support for RFC4122 UUID format feature to set RFC4122 encoding from build time produced by IPMICFG 1.29 tool or newer.</li></ol>

	<p><b>10. Set PCIe correctable and uncorrectable (non-fatal) error report to disabled by default.</b></p> <p><b>11. Disabled unused SPS ME "CUPS IIO" and "Volumetric Airflow" sensor.</b></p> <p><b>12. Set NVDIMM ADR timeout to 600us.</b></p> <p><b>13. Enhanced the solution for the error/warning message from dmidecode after a modification by AMIDE.</b></p> <p><b>14. Prevented inability to update BIOS when CMOS 51 value is 0x0a or 0x1a.</b></p>
<b>New features</b>	<b>N/A</b>
<b>Fixes</b>	<p><b>1. Fixed problem of BIOS always retrying boot when Re-Try Boot is Disabled.</b></p> <p><b>2. Fixed malfunction of support for LEGACY to EFI.</b></p> <p><b>3. Fixed failure of Always Turbo in Linux kernel 7.x.</b></p> <p><b>4. Fixed malfunction of CPU PBF (Prioritized Base Frequency).</b></p> <p><b>5. Fixed incorrect PBF high frequency core number when Hyper-Threading is disabled.</b></p> <p><b>6. Modified UEFI network description to IPv4/IPv6 to follow Industry Standard.</b></p> <p><b>7. Fixed issue of no AOC_SAS Temp when AOC-S3108L-H8iR is installed.</b></p>

## **Release Notes from Previous Release(s)**

### **2.1 (6/15/2018)**

1. Updated CPU microcode to address 'Spectre' derivatives (CVE-2018-3639 & CVE-2018-3640) security issue.
2. Changed BIOS revision to 2.1.
3. Updated 5.12\_PurleyCrb\_0ACFD088 for Purley Skylake platform PLR7, BKC 2018 WW20.
4. Updated BIOS ACM 1.3.7 and SINIT ACM 1.3.4.
5. Added one event log to record that the event log is full.
6. Added support for VMD settings to be preserved after flashing.
7. Updated SATA RAID OPROM/EFI driver to RSTe PreOS v5.4.0.1039.
8. Corrected BIOS/ME downgrade check for SPS 4.0.4.340.
9. Added support for UEFI mode PXE boot of F12 hot key Net boot.
10. Added setup item "SmcBusMasterEn" for enabling Parent bridge of the devices in the gSmcPciForceEnableBusMasterList.
11. Added support for SATA FLR.
12. Fixed problem of DMI being cleared when running SUM UpdateBios.
13. 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. Updated BIOS version to 2.0b.
3. Updated 5.12\_PurleyCrb\_0ACFD085Beta for Purley Skylake platform PLR 4, BKC WW02.
4. Displayed setup item "ACS Control" to Enable/Disable PCIe Access Control Services Extended Capability, with Enabled as default.
5. Disabled CPU2 IIO PCIe root port ACPI hot plug function.
6. Fixed issue with IPMI force boot.
7. Fixed malfunction of "SMBIOS Preservation" Disabled.
8. Fixed problem of SMC skipping first boot option in UEFI mode when retrying boot.
9. Fixed inability to reset the system under DOS by pressing "Ctrl-Alt-Del" on USB keyboard when "Port 60/64 Emulation" is disabled.
10. Fixed inability of some CPUs to display correct microcode revision under BIOS setup menu.
11. Fixed inability to detect 2 NVMe's with AOC 2E2T.
12. Fixed failure of SUM TC 219.