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	**X11SPH-NCTF/NCTPF**
Release Version	**3.1**
Release Date	**5/21/2019**
Previous Version	**3.0b**
Update Category	**Critical**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Changed BIOS version to 3.1.** **2. Updated Skylake-SP/Cascade Lake-SP CPU microcode for INTEL-SA-00233 Security Advisory.** **3. Updated to SPS 4.0.04.381 or above for INTEL-SA-00213 Security Advisory.** **4. Updated Intel BKCWW16 2019 PV PLR1.** **5. Updated SPS_E5_04.01.04.296.0 from BKC WW16 2019.** **6. Updated SATA/sSATA RAID OPROM/EFI driver to VROC PreOS v6.1.0.1017.** **7. Update EIP467272 for AMI SA50069, SA50070.** **8. Set SDDC Plus One or SDDC to disabled by default.** **9. Set Leaky Bucket that can decrease one memory correctable error count within 2.15 minutes with threshold 512.**

	10. Enhanced BIOS setup menu to auto-switch the Option ROM's value and hide the unexpected value when boot mode changes. 11. Updated to SPS 4.0.04.381 or above for INTEL-SA-00213 Security Advisory. 12. Set ADDDC Sparing to enable by default.
New features	**N/A**
Fixes	**1. Fixed inability to change IPv6 address or IPv6 Router1 IP address.** **2. Temporarily fixed error for SKX (CLX) 4114 CPU memory training with Micron (18ASF2G72PDZ-2G6E1) RDIMM.** **3. Fixed failure to boot into VMare OS when set to Maximum Performance, even if Monitor/MWAIT is enabled.**

Release Notes from Previous Release(s)

3.0b (3/04/2019)

1. Changed BIOS version to 3.0b.
2. Added support for Purley Refresh platform.
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.
4. Updated CPU microcode MB750654_0200005A for Skylake-SP H0/M0/U0 stepping CPUs.
5. Updated SATA RAID OPROM/EFI driver to RSTe PreOS v6.0.0.1024.
6. Added support for Monitor Mwait feature.
7. Fixed inability of VMD status to load default if loading default by AFU.
8. Added support for SMC HttpBoot.
9. Added support for RFC4122 UUID format feature to set RFC4122 encoding from build time produced by IPMICFG 1.29 tool or newer.
10. Set PCIe correctable and uncorrectable (non-fatal) error report to disabled by default.
11. Disabled unused SPS ME "CUPS IIO" and "Volumetric Airflow" sensor.
12. Set NVDIMM ADR timeout to 600us.
13. Enhanced the solution for the error/warning message from dmidecode after a modification by AMIDE.
14. Prevented inability to update BIOS when CMOS 51 value is 0x0a or 0x1a.
15. Fixed problem of BIOS always retrying boot when Re-Try Boot is Disabled.
16. Fixed malfunction of support for LEGACY to EFI.
17. Fixed failure of Always Turbo in Linux kernel 7.x.
18. Fixed malfunction of CPU PBF (Prioritized Base Frequency).
19. Fixed incorrect PBF high frequency core number when Hyper-Threading is disabled.
20. Modified UEFI network description to IPv4/IPv6 to follow Industry Standard.

2.1 (8/29/2018)

1. Updated CPU microcode to address 'Spectre' derivatives (CVE-2018-3639 & CVE-2018-3640) security issue.
2. Changed BIOS version 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 with enabled as default.
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.
14. Rolled back SVN_3413 to fix failure of WDT function.
15. Fixed problem of BIOS reporting incorrect SMBIOS Type 40 when device is installed on Slot 5 and no device is installed on Slot 6.
16. Fixed issue with IPMI firmware capability.

2.0b (2/26/2018)

1. Updated CPU microcode to address ‘Spectre’ variant 2 (CVE 2017-5715) security issue.
2. Changed BIOS revision to 2.0b.
3. Displayed setup item "ACS Control" to Enable/Disable PCIe Access Control Services Extended Capability, with Enabled as default.
4. Updated 5.12_PurleyCrb_0ACFD085Beta for Purley Skylake platform PLR 4, BKC WW02.
5. Added setup item "SmcBusMasterEn" for enabling Parent bridge of the devices in the gSmcPciForceEnableBusMasterList.
6. Fixed failure of BIOS ECO ATT test case 306.
7. Fixed inability to reset the system under DOS by pressing "Ctrl-Alt-Del" on USB keyboard when "Port 60/64 Emulation" is disabled.
8. Fixed problem of SMC skipping first boot option in UEFI mode when retrying boot.
9. Disabled CPU2 IIO PCIe root port ACPI hot plug function.
10. Fixed issue with IPMI force boot.
11. Fixed inability of some CPUs to display correct microcode revision under BIOS setup menu.