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	**X11DPT-B(H)**
Release Version	**3.0c SPS: 4.1.04.256**
Release Date	**3/30/2019**
Previous Version	**3.0a**
Update Category	**Recommended**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Updated Intel BKCWW12 2019 PV MR4.** **2. Updated SPS_E5_04.01.04.256.0 from BKC WW08 2019.** **3. Updated SINIT ACM 1.7.2 PW from BKC WW06 2019.** **4. Updated Skylake-SP/Cascade Lake-SP CPU microcode from SRV_P_272.** **5. Added driver health warning message.** **6. Hid Driver Health page for SUM.** **7. Reduced redundant reboot for offboard VGA switching.** **8. Set NVDIMM ADR timeout to 600µs.** **9. Enhanced the solution for the error/warning message from dmidecode after a modification by AMIDE.** **10. Improved behavior of "Monitor/MWAIT" & "Extreme/Maximum Performance".** **11. Updated to SPS 4.1.02.174 or above for INTEL-SA-00185 Security**

	Advisory and to RC 549.D13 or above for INTEL-SA-00192 Security Advisory. 12. Enhanced BIOS setup menu to auto-switch the Option ROM's value and hide the unexpected value when boot mode changes. 13. Enhanced BIOS setup menu to switch the boot mode value and Option ROM's values when CSM support is disabled and applied this to enabled secure boot mode case. 14. Enable SDDC+1/ADDDC by default
New features	N/A
Fixes	1. Fixed problem of the system equipped with dTPM 2.0 hanging up at POST code 0x90 when disabling dTPM 2.0 by SUM TPM OOB command "--disable_dtpm". 2. Corrected TPM RSD ChangeTPMState behavior to control TPM 1.2/2.0 state instead of "Security Device Support". 3. Fixed problem of TPM 2.0 device disappearing when disabling "RSD PSME ChangeTPMState API" and then enabling TPM 2.0 state. 4. Modified UEFI network description to IPv4/IPv6 to follow Industry Standard. 5. Fixed problems of system hanging up at POST code 0x92 and rebooting endlessly during POST and inability to get PPIN under OS (DOS/EFI shell/Windows/Linux). 6. Fixed failure of NVMe hotplug function with BPN-ADP-12NVMe-2UB under Linux OS. 7. Fixed failure to log memory UCE event due to incorrect flag. 8. Fixed inability of "Network Stack"-related items to get/change via SUM OOB method. 9. Fixed incorrect display of the TDP of Intel Speed Select table. 10. Patched problem of incorrect memory power being reported in

	PTU. **11. Applied workaround for inability of SUM to get full setting of IODC setup item.** **12. Temporarily fixed error for SKX (CLX) 4114 CPU memory training with Micron (18ASF2G72PDZ-2G6E1) RDIMM.**

Release Notes from Previous Release(s)

3.0a (2/20/2019)

1. Added support for Purley Refresh platform.
2. Updated SATA RAID OPROM/EFI driver to RSTe PreOS v6.0.0.1024.
3. Updated Giga LAN legacy PXE/legacy iSCSI OPROM driver to IBA 23.2 and uEFI driver to IBA 23.5.
4. Set BMC MAC address to UUID for system without onboard LAN1 or with onboard LAN1 disabled.
5. Set PCIe correctable and uncorrectable (non-fatal) error report to disabled by default.
6. Set RFC4122 encoding to only be enabled for build time produced by IPMI 1.29 or newer.
7. Updated CPU microcode SRV_P_264 for Skylake-SP H0/M0/U0 CPUs.
8. Updated valid range of IPMI setup item VLAN ID to 1-4094.
9. Added support for "Extreme Performance Mode" with 2U2Node backplane adapters.
10. Fixed problem of setup item "Quiet Boot" staying enabled after flashing BIOS with "Quiet Boot" disabled.

2.1a (9/15/2018)

1. Set PCIe link status to be polled at DXE stage to fix wrong information in BIOS setup IIO page.
2. Disabled "tRWSR Relaxation" by default.
3. Added support for Monitor Mwait feature.
4. Updated SPS 4.0.4.381 for INTEL-SA-00131 Security Advisory to address CVE-2018-3643 and CVE-2018-3644 security issues.
5. Fixed inability of VMD status to load default if loading default by AFU.
6. Updated CPU microcode SRV_P_253 for Skylake-SP H0/M0/U0 stepping CPUs.
7. Fixed missing sensor reading for add-on devices.
8. Fixed problem of BIOS always retrying boot when Re-Try Boot is Disabled.
9. Fixed malfunction of BIOS/ME downgrade check when running flash package (SWJPME2) a second time.
10. Fixed problem of system resetting while flashing BIOS under OS if Watch Dog function is enabled.
11. Fixed missing information for Hybrid backplane SMBIOS type 39.
12. Fixed failure of turbo in new Linux kernel.

2.1 (7/13/2018)

1. Updated CPU microcode to address 'Spectre' derivatives (CVE-2018-3639 & CVE-2018-3640) security issue.
2. Updated 5.12_PurleyCrb_0ACFD088 for Purley Skylake platform PLR7, BKC 2018 WW20.
3. Updated Giga LAN EFI driver 8.3.0.4 (IBA 23.1).
4. Updated SPS 4.00.04.340 PV PLR7 version.
5. Updated SATA RAID OPROM/EFI driver to RSTe PreOS v5.4.0.1039.
6. Corrected default setting for Enable SmcBusMasterEn setup item.
7. Corrected BIOS/ME downgrade check for SPS 4.0.4.340.
8. Added support for UEFI mode PXE boot of F12 hot key Net boot.
9. Added one event log to record that the event log is full.
10. Updated BIOS ACM 1.3.7 and SINIT ACM 1.3.4.
11. Fixed problem of SUM GetSataInfo showing incorrect "Configuration Type" when setting "Configure sSATA as" to "AHCI" or "RAID" on sSATA controller.
12. Fixed problem of Ctrl + Alt + Del causing system to hang after flashing BIOS.
13. Fixed missing NVDIMM ADR setup item.
14. Fixed problem of system hanging when installing Linux OS after COM1 & COM2 IO/IRQ exchange.

2.0b (2/24/2018)

1. Updated CPU microcode to address CVE-2017-5715 security patch issue.
2. Updated 5.12_PurleyCrb_0ACFD085Beta for Purley Skylake platform PLR 4, BKC WW02.
3. Added setup item "SmcBusMasterEn" for enabling Parent bridge of the devices in the gSmcPciForceEnableBusMasterList.
4. Changed RC default setting to upgrade POST Memory correctable error to uncorrectable error and map out the channel.
5. Added support for System Firmware Progress System Firmware Progress feature.
6. Fixed inability to reset the system under DOS by pressing "Ctrl-Alt-Del" on USB keyboard when "Port 60/64 Emulation" is disabled.
7. Fixed problem of SMC skipping first boot option in UEFI mode when retrying boot.
8. Fixed malfunction of "SMBIOS Preservation" Disabled.
9. Fixed issue of all commands requesting to be persistent.
10. Disabled CPU2 IIO PCIe root port ACPI hot plug function.
11. Fixed issue with IPMI force boot.
12. Fixed malfunction of option ROM control for AOC-MTG-i2TM and BPN-ADP-12NVMe-2UB.
13. Fixed problem of system hanging during BIOS flashing if Watch Dog function is enabled.
14. Fixed problem of the system not logging memory errors upon injection without rebooting.
15. Fixed incorrect LED behavior if VMD is disabled by stack but not by ports.