

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-PS
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	<ol style="list-style-type: none">1. Updated Intel BKCWW10 2019 PV MR3.2. Updated SPS_E5_04.01.04.256.0 from BKC WW08 2019.3. Updated Skylake-SP/Cascade Lake-SP CPU microcode from SRV_P_272.4. Set PCIe correctable and uncorrectable (non-fatal) error report to disabled by default.5. Disabled unused SPS ME "CUPS IIO" and "Volumetric Airflow" sensor.6. Added support for Linux built-in utility efibootmgr.7. Updated valid range of IPMI setup item VLAN ID to 1-4094.8. Enhanced BIOS setup menu to auto-switch the Option ROM's value and hide the unexpected value when boot mode changes.9. 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.

	<p>10. Changed OPROM settings to EFI to correct behavior of the OEM BIOS with the boot mode changed to UEFI without other changes.</p> <p>11. Set SDDC+1/ADDDC to enabled by default.</p>
New features	N/A
Fixes	<p>1. Fixed failure of CPU PBF (Prioritized Base Frequency).</p> <p>2. Added workaround for failure of BIOS flash with 156 bytes PubKey (Error: "Secure Flash Rom Verify Fail").</p> <p>3. Modified UEFI network description to IPv4/IPv6 to follow Industry Standard.</p> <p>4. Fixed malfunction of AOC-MTG-i2T SIOM sensor and OPROM control.</p> <p>5. Applied workaround for inability of SUM to get full setting of IODC setup item.</p> <p>6. Fixed failure to boot into VMware OS when set to Maximum Performance even if Monitor/MWAIT is enabled.</p> <p>7. Temporarily fixed error for SKX (CLX) 4114 CPU memory training with Micron (18ASF2G72PDZ-2G6E1) RDIMM.</p>

Release Notes from Previous Release(s)

3.0a (1/12/2019)

1. Added support for Purley Refresh platform.
2. Updated SATA RAID OPROM/EFI driver to RSTe PreOS v6.0.0.1024.
3. Added support for Monitor Mwait feature.
4. Patched missing PSU information if backplane MCU reports wrong PSU information.
5. Added SIOM add-on card back to SMBIOS Type 41 to handle Linux OS network configuration case.
6. Set BMC MAC address to UUID for system without onboard LAN1 or with onboard LAN1 disabled.
7. Hid setup item "L2 RFO Prefetch Disable" to adhere to draft template v0.7.
8. Changed BIOS revision to 3.0a.
9. Enabled RFC4122 UUID support.
10. Fixed malfunction of disabling Watch Dog while flashing BIOS under OS.
11. Fixed problem of BIOS always retrying boot when Re-Try Boot is Disabled.
12. Fixed malfunction of support for LEGACY to EFI.
13. Fixed failure of always turbo in new Linux kernel 7.x.
14. Fixed problem of system hanging and falling into a dead loop when setting enabled CPU core number to 1 in always turbo mode.
15. Fixed problem of CPU core numbers and maximum turbo ratio not matching in always turbo mode.
16. Fixed failure of CPU PBF (Prioritized Base Frequency).

2.1 (8/23/2018)

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 Giga LAN EFI driver 8.3.0.4 (IBA 23.1).
4. Added 1T option for MMIO High Base setup item.
5. Added BIOS/ME downgrade check for SPS 4.0.4.381.
6. Changed maximum speed in SMBIOS type 4 to 4500Mhz.
7. Added one event log to record that the event log is full.
8. Added support for SATA FLR.
9. Displayed PPR setup item.
10. Added a patch to prevent reboot hang when installing AVAL APX-3224 card.
11. Moved SIOM SMBIOS definition from type 41 to type 9.
12. Exported driver health menu under setup.
13. Added support for full function of AOC-MHIBE-M1CGM SIOM.
14. Fixed problem of Ctrl + Alt + Del causing system to hang after flashing BIOS.
15. Fixed problem of some NVDIMM items not appearing in setup menu.
16. Fixed incorrect VPD data and oversized string to prevent system from hanging.
17. Fixed problem of system hanging when installing Linux OS after COM1 & COM2 IO/IRQ exchange.
18. Fixed problem of SUM GetSataInfo showing incorrect "Configuration Type" when setting "Configure sSATA as" to "AHCI" or "RAID" on sSATA controller.
19. Fixed issue with IPMI firmware to enable storage card to show temperature.

2.0b (2/24/2018)

1. Updated CPU microcode to address CVE-2017-5715 security patch issue.
2. Updated Purley RC 151.R03.
3. Changed RC default setting to upgrade POST Memory correctable error to uncorrectable error and map out the channel.

4. Patched for inability of AOC-MH25G-b2S2G to show sensor.
5. Disabled CPU2 IIO PCIe root port ACPI hot plug function.
6. Fixed inability of AOC-MTG-i4T to show sensor.
7. Fixed problem of SMC skipping first boot option in UEFI mode when retrying boot.
8. Fixed inability to reset the system under DOS by pressing "Ctrl-Alt-Del" on USB keyboard when "Port 60/64 Emulation" is disabled.
9. Fixed inability of some CPUs to display correct microcode revision under BIOS setup menu.

2.0 (11/30/2017)

1. Changed BIOS revision to 2.0.
2. Updated Purley RC 149.R09, SPS 4.0.04.294, ACM files, and CPU microcode.
3. Set message "BIOS cannot support downgrade to previous version or ROMID mismatch" to show when trying to downgrade BIOS or flash other model of BIOS.
4. Fixed problem of serial console output showing SMC logo when EarlyVideo logo item is disabled.
5. Fixed problem of the Last UCE report (mapout) DIMM sometimes not matching real UCE DIMM location.
6. Fixed problem of IPMI SEL logging "Memory training failure." and "No memory DIMM detected, install memory DIMMs." twice per reboot.
7. Fixed problem of TPM 1.2 PS index not being Write-Protected so that the content of TPM 1.2 PS index still can be modified after TPM 1.2 is nvLocked.
8. Fixed problem of changes to CPU core Enable/Disable in setup menu sometimes not taking effect on Windows OS.
9. Fixed problem of system hanging during BIOS flashing if Watch Dog function is enabled.
10. Fixed system reboots endlessly when equipping dTPM module.
11. Fixed inability of DMI Customized Information to preserve after user implements BIOSLoadDefault or CMOS Clear Action.