

## 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>X11DPG-QT</b>
<b>Release Version</b>	<b>3.0b for X11DPG9.305_32MB and X11DPG9.305</b>
<b>Release Date</b>	<b>03/05/2019</b>
<b>Previous Version</b>	<b>3.0a</b>
<b>Update Category</b>	<b>Critical</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. Added support for Purley Refresh platform.</li><li>2. Updated CPU microcodes from SRV_P_270.</li><li>3. Updated SINIT ACM 1.7.2 PW from BKC WW06 2019.</li><li>4. Updated SPS_E5_04.01.04.251.0 from Intel VIP Kit #130885.</li><li>5. Added support for Linux built-in utility efibootmgr.</li><li>6. Updated IPv6 router-related setup item string.</li><li>7. Reduced redundant reboot for offboard VGA switching.</li><li>8. Set NVDIMM ADR timeout to 600us.</li><li>9. Enabled support for Thunderbolt 2.0.</li><li>10. 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></ol>
<b>New features</b>	<b>N/A</b>

<b>Fixes</b>	<ol style="list-style-type: none"><li><b>1. Modified UEFI network description to IPv4/IPv6 to follow Industry Standard.</b></li><li><b>2. Patched problem of system hanging at 0x94 when plugging in Nvidia Tesla T4 card.</b></li><li><b>3. Fixed inability of "Network Stack"-related items to get/change via SUM OOB method.</b></li></ol>
--------------	---

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

### **3.0a (12/21/2018)**

1. Updated 5.14\_PurleyCrb\_OACLA031\_BETA for Purley Skylake platform, BKC 2018 WW36.
2. Added support for Monitor Mwait feature.
3. Fixed inability of VMD status to load default if loading default by AFU.
4. Added support for SMC HttpBoot.
5. Fine tuned function code of "Install Windows 7 USB Support" setup item.
6. Removed support for S3 due to SPS ME limitation.
7. Removed support for Thunderbolt.
8. Skipped downgrade of BIOS to 2.x when using next generation CPU.
9. Added support for NVMe auto detection with SMC NVMe add-on card on slot 2/4/6/8/9/10.
10. Added support for Purley Refresh platform.
11. Updated SATA RAID OPROM/EFI driver to RSTe PreOS v6.0.0.1024.
12. Set PCIe correctable and uncorrectable (non-fatal) error report to disabled by default.
13. Set RFC4122 encoding to only be enabled for build time produced by IPMI 1.29 or newer.
14. Updated CPU microcode SRV\_P\_262 for Skylake-SP H0/M0/U0 CPUs.
15. Disabled unused SPS ME "CUPS IIO" and "Volumetric Airflow" sensor.
16. Fixed problem of BIOS always retrying boot when Re-Try Boot is Disabled.
17. Fixed malfunction of support for LEGACY to EFI.
18. Fixed failure of always turbo in new Linux kernel 7.x.
19. Fixed problem of system hanging and falling into a dead loop when setting enabled CPU core number to 1 in always turbo mode.
20. Fixed problem of CPU core numbers and maximum turbo ratio not matching in always turbo mode.
21. Fixed problem of setup item "Quiet Boot" staying enabled after flashing BIOS with "Quiet Boot" disabled.

### **2.1 (7/20/2018)**

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. Added support for SATA FLR.
9. Fixed problem of SUM GetSataInfo showing incorrect "Configuration Type" when setting "Configure sSATA as" to "AHCI" or "RAID" on sSATA controller.
10. Fixed problem of Ctrl + Alt + Del causing system to hang after flashing BIOS.
11. Fixed problem of system hanging when installing Linux OS after COM1 & COM2 IO/IRQ exchange.
12. Fixed failure of WDT function.
13. Added workaround for low GPU P2P bandwidth.

### **2.0b (4/18/2018)**

1. Updated CPU microcode to address 'Spectre' variant 2 (CVE 2017-5715) security issue.
2. Enabled IERR crash dump function.
3. Added setup item "SmcBusMasterEn" for enabling Parent bridge of the devices in the gSmcPciForceEnableBusMasterList.

4. Updated 5.12\_PurleyCrb\_0ACFD085Beta for Purley Skylake platform PLR 4, BKC WW02.
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. Added support for M/B 1.10A with 32MB BIOS chip.
8. Implemented SMC OOB TPM Provisioning via IPMI Feature for customized provisioning table.
9. Changed RC default setting to upgrade POST Memory correctable error to uncorrectable error and map out the channel.
10. Fixed problem of yellow marked device appearing in Windows device manager after S3 resumes.
11. Corrected the "Save Changes" setup option string in "Save & Exit" menu.
12. Disabled SNC once NVDIMM is present in system.
13. Fixed problem of system hanging during BIOS flashing if Watch Dog function is enabled.
14. 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".
15. Fixed problem of system rebooting endlessly when equipping dTPM module.
16. Fixed problem of DMI being cleared when running SUM LoadDefaultBiosCfg.
17. Fixed problem of some platforms hanging up at POST code 0xB2 when equipping dTPM module.
18. Fixed inability of BIOS to boot into OS with Intel P3608 PCIe NVMe drive installed.
19. Disabled CPU2 IIO PCIe root port ACPI hot plug function.
20. Fixed issue with IPMI force boot.
21. Fixed issue of all commands requesting to be persistent.
22. Fixed malfunction of "SMBIOS Preservation" Disabled.
23. Fixed problem of SMC skipping first boot option in UEFI mode when retrying boot.
24. Fixed problem of the endpoint PCIe device having error bits in PCI Status or Device Status register.
25. Fixed inability to set memory policy.
26. Fixed inability to reset the system under DOS by pressing "Ctrl-Alt-Del" on USB keyboard when "Port 60/64 Emulation" is disabled.
27. Fixed failure of BIOS ECO ATT test case 306.
28. Fixed inability of some CPUs to display correct microcode revision under BIOS setup menu.
29. Fixed failure of SATA HSIO register setting test.