

## IPMI Firmware / BIOS Release Notes Form

*Super Micro 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. Super Micro and the Super Micro logo are trademarks of Super Micro Computer, Inc. in the U.S. and/or other countries. Copyright © 2017 Super Micro Computer, Inc. All rights reserved.*

<b>Product Name</b>	<b>X11DPG-QT</b>
<b>Release Version</b>	<b>2.0</b>
<b>Release Date</b>	<b>11/29/2017</b>
<b>Previous Version</b>	<b>1.0</b>
<b>Update Category</b>	<b>Critical</b>
<b>Dependencies</b>	<b>None</b>
<b>Important Notes</b>	<b>N/A</b>
<b>Enhancements</b>	<ol style="list-style-type: none"><li>1. Enabled display of EarlyVideo message by onboard video when VGA Priority is set to Offboard.</li><li>2. Removed the "System Firmware Error (POST ERROR)" error log from BMC and "EFI 01030006" in BIOS event log.</li><li>3. Added support for M.2 slot (PCIe M.2).</li><li>4. Updated 5.12_PurleyCrb_0ACFD083_BETA for Purley Skylake Platform BKC WW39.</li><li>5. Updated SPS 4.00.04.288 PLR version for security vulnerabilities.</li><li>6. Updated BMC LAN configuration for saving settings of BIOS setup menu.</li><li>7. Set to avoid TCG protocol "PassThroughToTpm" failure under EFI shell when user enables "TXT Support" with disabled "TPM state" in TPM 1.2 BIOS setup menu.</li><li>8. Changed BIOS revision to 2.0.</li></ol>

	<p>9. Updated help string for tCCD relax setup option.</p> <p>10. Updated CPU microcode SRV_P_211 for Skylake-EP H0 stepping CPUs.</p> <p>11. Corrected help string of setup item "Enforce POR".</p> <p>12. Updated new MRC error log definition.</p> <p>13. Allowed runtime memory UCE mapout message to be displayed one time during BIOS POST.</p> <p>14. Increased SataRaidOromDelay &amp; SataRaidOromDelay to 6 seconds.</p> <p>15. Updated ShellBinPkg_08 for CapsLock/NumLock malfunction.</p> <p>16. Reduced the boot time caused by IPv4/IPv6 polling.</p> <p>17. Added "SMBIOS Preservation" Enabled/Disabled item for flash recovery.</p> <p>18. Masked off PCIe correctable and non-fatal errors.</p> <p>19. Set PCIe correctable error to not log and legacy PCI PERR or SERR error to still log.</p> <p>20. Removed PCI PERR/SERR Support item and enabled reporting PCIe error by default.</p> <p>21. Hid "IPMI" and "Secure Boot" forms for SUM.</p>
New features	<p>1. Removed support for Ctrl+home triggering recovery.</p> <p>2. Set display of setup option for always turbo mode function as default.</p> <p>3. Exported "IMC Interleaving" item for performance tuning.</p> <p>4. Displayed "PCIe PLL SSC" setup item for clock spectrum function.</p> <p>5. Added the "PEI--IPMI Initialization" Post-Help message.</p> <p>6. Added setup item for Samsung tRWSR.</p> <p>7. Displayed setup item "Core Disable Bitmap(Hex)" in BIOS CPU Configuration page.</p> <p>8. Implemented SMC Recovery Flash Boot Block Feature.</p> <p>9. Set BIOS/ME flashing to be skipped when trying to downgrade the SPS ME firmware from 4.0.4.288 to previous version.</p> <p>10. Set message "BIOS cannot support downgrade to previous version"</p>

	<p>or ROMID mismatch" to show when trying to downgrade BIOS or flash other model of BIOS.</p>
Fixes	<ol style="list-style-type: none"> <li>1. Fixed problem of "Correctable, Non-Fatal and Fatal" error reporting flags being disabled on "Infiniband controller: Mellanox Technologies MT27700 Family [ConnectX-4]" when "PCI PERR/SERR Support" is enabled.</li> <li>2. Fixed inability of the system to enter TXT Environment when using TPM 1.2 on production platform.</li> <li>3. Fixed problem of TPM 2.0 BIOS-Based Provisioning table not setting PW flag to PS LCP Data for production platform.</li> <li>4. Corrected USB 2.0 and 3.0 mapping table for WHQL.</li> <li>5. Fixed failure of setup item "Install Windows 7 USB support".</li> <li>6. Corrected SMBIOS Type 9/40 information for CPU1 PCIe slot.</li> <li>7. Fixed failure of Password Preservation Test due to password not being preserved.</li> <li>8. Fixed problem of the string of "Error DIMM information" on screen being corrupted when equipping failed DIMM.</li> <li>9. Fixed problem of system shutting down automatically at post code 0xEE when power button is used to power off and power on system.</li> <li>10. Fixed problem of system sometimes hanging at post code B2 when running Cburn ONOFF.</li> <li>11. Fixed inability to enter setup menu when pressing "DEL" key if there is no boot device.</li> <li>12. Fixed problem of SUM GetDmiInfo command error "Invalid DMI information from BIOS" occurring.</li> <li>13. Fixed malfunction with SMCSataFrozen item.</li> <li>14. Fixed failure of SMBIOS Type 20 to fill Interleave Position and Interleaved Data Depth correctly.</li> <li>15. Fixed problem of PCIe device behind CPU2 PCIe root port dropping after enabling "IIO/PCH Global Error Support" (IioErrorEn) and "IIO LER</li> </ol>

	<p>Support" (LerEn) and then doing a warm reset.</p> <p>16. Fixed problem of system hanging when set to NVMe VMD mode for CPU PCIe Root Port.</p> <p>17. Fixed BMC PCIe root port being forced to Gen1.</p> <p>18. Fixed problem of the Runtime Uncorrectable Memory error injection causing system to enter into endless reboot at POST code 0xEE.</p> <p>19. Fixed the Endless reboot caused by Last-time-uncorrected-memory error.</p> <p>20. Fixed inability of Intel RC Setup strings to appear in SUM BIOS CFG file when booting to OS directly.</p> <p>21. Fixed problem of serial console output showing SMC logo when EarlyVideo logo item is disabled.</p> <p>22. Fixed problem of the Last-runtime-memory-UCR causing system to hang at POST 0x79.</p> <p>23. Fixed problem of the Last UCR report (mapout) DIMM sometimes not matching real UCR DIMM location.</p> <p>24. Corrected Hynix DIMM info to "SK Hynix".</p> <p>25. Fixed problem of system repeatedly rebooting when SUM runs Test Case #216, #219, or #413 while memory (32GB*12) is plugged in.</p> <p>26. Fixed inability of system to log correct DIMM.</p> <p>27. Fixed problem of IPMI SEL logging "Memory training failure." and "No memory DIMM detected, install memory DIMMs." twice per reboot.</p> <p>28. Fixed inability of USB wake to disable when setup item "Real USB Wake Up" or "Front USB Wake Up" is disabled.</p> <p>29. 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.</p> <p>30. Fixed problem of system hanging when using AFUWIN/AFULNX to flash BIOS under OS.</p>
--	--

	<p><b>31. Fixed problem of changes to CPU core Enable/Disable in setup menu sometimes not taking effect on Windows OS.</b></p> <p><b>32. Fixed problem of yellow mark device being present in Windows device manager after S3 resumes.</b></p> <p><b>33. Fixed run SUM LoadDefaultBiosCfg but DMI is cleared too.</b></p>
--	---

*Release Notes from Previous Release(s) – these will be appended at the bottom of the current release notes in italic and in smaller print*

--