

# **Notes to Release Notes Authors**

- All fields must be completed; please indicate as “N/A” if not applicable.
- Release Notes should document functional changes, dependencies, bug fixes and added features.
- Release Notes must not mention the methods of implementation and/or internal processes.
- Release Notes must not mention of silicon errata and/or other external causations.
- Release Notes must not mention confidential/proprietary information and/or trade secrets of Supermicro or any third party.
- Please delete this page and the signature fields before submitting the document in PDF Format to Marketing for publication.

## 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>X10QBL(-CT/4/4CT)</b>
<b>Release Version</b>	<b>3.1</b>
<b>Release Date</b>	<b>7/20/2018</b>
<b>Previous Version</b>	<b>3.0b</b>
<b>Update Category</b>	<b>Recommended</b>
<b>Dependencies</b>	<b>None</b>
<b>Important Notes</b>	<b>None</b>
<b>Enhancements</b>	<b>1. Updated CPU microcode to address 'Spectre' derivatives (CVE-2018-3639 &amp; CVE-2018-3640) security issue.</b> <b>2. Updated BIOS version to 3.1.</b> <b>3. Added temperature sensor reading support for AOC-STGS-i2T and AOC-STG-I4S.</b> <b>4. Removed "2-Way Node Interleaving" and "8-Way Interleaving, inter-socket", and set "4-Way Node Interleaving" as default setting of Memory Interleaving feature in BIOS setup menu.</b> <b>5. Implemented "SMBIOS Preservation" Enabled/Disabled item for flash recovery.</b>
<b>New features</b>	<b>N/A</b>

Fixes	<ol style="list-style-type: none"> <li>1. Fixed incorrect FID minor version when BIOS version is "3.1".</li> <li>2. Fixed problem of Afu /O command clearing SMC SMBIOS region (\$SMC).</li> <li>3. Fixed failure to change DMI after updating BIOS with flash_smbios.</li> <li>4. Fixed failure to check HDD information in BMC that results in "Completion code is not zero" error.</li> <li>5. Added workaround for issue of unexpected system behavior while reading the same 4Kbyte physical memory.</li> <li>6. Fixed failure to flash BIOS with Watchdog.</li> <li>7. Fixed the issue of UEFI Boot option becoming "Disabled" if HDD is re-plugged in with UEFI Windows on its native installation environment.</li> <li>8. Set B:D.F 00:31.0 + 0xDC bit[01] BLE = 1 (BIOS Lock Enable), bit[05] SMM_BWP = 1 (SMM BIOS Write Protection).</li> <li>9. Fixed security issue with checking EFI/Tiano decompress bounds mentioned in UEFI Mantis 201802-001 issue #2.</li> <li>10. Fixed security issue with logic error in FV parsing mentioned in UEFI Mantis 201802-001 issue #4.</li> <li>11. Fixed failure of NM P-state control function under UEFI OS.</li> </ol>
-------	--

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

***3.0b (3/1/2018)***

- 1. Changed BIOS revision to 3.0b.*
- 2. Updated BDX-EX RC Package to 3.9.0.*
- 3. Updated Intel BIOS ACM v4.1.0 and SINIT ACM to v4.0.4.*
- 4. Updated Broadwell-EX B-0 stepping microcode to MEF406F1\_0B00002A, Haswell-EX E-0 stepping microcode to M80306F4\_00000011, and IvyBridge-EX D-1 stepping microcode MED306E7\_00000713.*
- 5. Fixed issue of IPMI LAN status being incorrect when using IPMI WebGUI or command to change LAN source.*
- 6. Fixed missing Generic ELOG Protocol.*
- 7. Fixed failure to restore BIOS setting to default when BIOS doesn't clear CMOS via IPMI command.*
- 8. Fixed corruption of BIOS ACPI table in the Main Block.*
- 9. Fixed inability to change OPRAM NVRAM setting with tool.*
- 10. Fixed inability of DDD3/DDR4 speed ratio to meet Intel Brickland memory POR.*
- 11. Fixed inability of VPD data to find VB tag.*
- 12. Fixed inability of system to enter recovery mode when MAIN block is updated and then system powers off.*

---

*Product Manager*

---

*Date*