

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	X10DRT-B
Release Version	3.1c SPS: 3.1.3.72
Release Date	04/27/2019
Previous Version	3.1a
Update Category	Recommended
Dependencies	None
Important Notes	None
Enhancements	1. Updated Intel Server Platform Services 3.1.3.72 for Grantley Refresh Platforms. 2. Updated SATA/sATA RAID OPRM/EFI driver to VROC PreOS v6.1.0.1017. 3. Updated VBIOS and VGA EFI Driver to 1.09 to fix ASpeed CVE-2019-6260 security issue. 4. Updated Haswell-EP/Broadwell-EP CPU microcode from SRV_P_273 for INTEL-SA-00233. 5. Updated valid range of IPMI setup item VLAN ID to 1-4094. 6. Added support for RFC4122 UUID format feature to set RFC4122 encoding from build time produced by IPMICFG 1.29 tool or newer. 7. Added support for setting IPv6 Static Router1 prefix length and value in BIOS setup menu feature.

New features	N/A
Fixes	1. Displayed the driver health support pages to support LSI (Broadcom 9440-8i) driver health status. 2. Fixed malfunction of Windows Consistent Device Naming (CDN). 3. Corrected UUID with LAN chips like X710 and Mellanox.

Release Notes from Previous Release(s)

3.1a (10/6/2018)

1. Forced a global reset if SPI descriptor is not write-protected after BIOS flash.
2. Implemented anti-rollback for FDT Read-Only.
3. Implemented multi-line IPMI page text and string.
4. Updated EIP393007 & EIP411789 for TPM vulnerability when resuming S3.
5. Updated CPU microcode for PC6 issue.
6. Fixed problem of BIOS always retrying boot when Re-Try Boot is Disabled.
7. Fixed malfunction of METW if many error events are triggered within a very short time.

3.1 (6/13/2018)

1. Updated CPU microcode to address 'Spectre' derivatives (CVE-2018-3639 & CVE-2018-3640) security issue.
2. Added support for IPMI IPV6.
3. Removed unsupported memory frequency options from setup menu.
4. Disabled Cloaking for Broadwell E5-2687W V4 CPU (W: workstation SKU).
5. Enhanced CPU1 SLOT SI tuning for better PCIe margin.
6. Updated Broadwell-EP RC 4.4.0 release.
7. Fixed problem of Afu /O command clearing SMC SMBIOS region (\$SMC).
8. Fixed problem of SUM OOB GetSataInfo always showing "Configuration Type" as "AHCI" when setting "Configure SATA as" to "RAID" or "IDE".
9. Fixed inability to enter setup menu by pressing "DEL" key if Re-try Boot feature is enabled and there are no boot devices.
10. Fixed redundant NVMe temperature in IPMI sensor reading for "BPN-ADP-6NVMe3-1UB".
11. Set Descriptor Region of BIOS Region Write Access to "No".

3.0a (02/13/2018)

1. Implemented enhancement to address 'Spectre' variant 2 (CVE 2017-5715) security patch issue.
2. Updated Broadwell-EP RC 4.3.0 PLR11 release.
3. Updated Intel Server Platform Services 3.1.3.50 for Grantley Refresh Platforms.
4. Set graphic mode as 1024x768 resolution and SMC Logo as 800x600 resolution.
5. Updated SATA RAID OPROM/EFI driver to RSTe PreOS v4.7.0.1014 (RSTe SATA 4.7.0.1069 and NVMe 4.7.0.2063).
6. Enabled use of Ctrl+R hotkey from remote console for LSI RAID card.
7. Added tCCD_L Relaxation item under Memory Configuration menu.
8. Displayed setup item "ACS Control" to Enable/Disable PCIe Access Control Services Extended Capability.
9. Updated BIOS ACM 3.1.1 PW and SINIT ACM 3.1.1 PW.
10. Added SumBbsSupportFlag into DAT file.
11. Removed SIOM report for SMBIOS type 41 so that SIOM only reports on SMBIOS type 9.
12. Implemented dynamic update of SMBIOS type 9 for different backplane and riser.
13. Added "SMBIOS Preservation" Enabled/Disabled item for flash recovery.
14. Enhanced SMC Recovery Flash Boot Block feature.
15. Fixed inability of SUM to get COM2/SOL settings from BIOS.
16. Fixed inability of SUM utility to get "Setup Prompt Timeout" setup item.
17. Changed Memory correctable threshold to 100 and enabled Cloaking for Broadwell CPU E5-26xx SKU.
18. Implemented Dynamic MMCFG BASE feature.

19. Added new support for backplane adapter cards.
20. Added support for JEDEC NVDIMM.
21. Added support for AOC-SLG3-2M2 auto bifurcation on CPU1 SXB1 SLOT.
22. Implemented SMC Recovery Flash Boot Block Feature, adding message to inform user with the POST screen message, "The System Is Going To Reset And Then Entering To Recovery Mode Again..."
23. Added support for System Firmware Progress feature.
24. Fixed multiple event time count not following the specifications.
25. Fixed problem of IPMI boot command being cleared even when persistence boot has been set.
26. Fixed issue of power button not being reported in ACPI table when set to "4 Seconds Override".
27. Fixed inability of the system to boot at debug card showing 00h after over 50% of boot block is erased and JBR1 is set to pins 2-3 (BIOS RECOVERY).
28. Fixed failure of BIOS Auto Recovery.
29. Fixed problem of system resetting or hanging after Watch Dog function is enabled during BIOS update.
30. Fixed issue of Super.rom not working and SUT hanging on POST 79.
31. Fixed problem of NVDIMM setup items appearing when optimized defaults load even without NVDIMM being installed.
32. Fixed problem of MWAIT being disabled on BSP only.
33. Fixed inability to get correct Memory CECC DIMM location via SD5.
34. Fixed problem of SMBIOS Type4 CPU2 current speed not showing as zero when CPU2 is not installed.
35. Fixed problem of system hanging at POST 0xA9 when entering setup menu while Intel P4800X uEFI driver is loaded.
36. Updated FlashDriver module to Label 5 in order to fix inability of system to enter recovery mode when MAIN block is updated 45% and then system powers off.