IPMI Firmware / BIOS Release Notes Form

Product Name	**X10DRT-PS**
Release Version	**3.1a**
Release Date	**10/6/2018**
Previous Version	**3.1**
Update Category	**Recommended**
Dependencies	**None**
Important Notes	**None**
Enhancements	**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.**
New features	**N/A**
Fixes	**1. Fixed problem of BIOS always retrying boot when Re-Try Boot is Disabled.** **2. Fixed malfunction of METW if many error events are triggered within a very short time.**

Release Notes from Previous Release(s)

3.1 (6/9/2018)

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. Updated Broadwell-EP RC 4.4.0 release.
5. Fixed problem of Afu /O command clearing SMC SMBIOS region ($SMC).
6. Fixed problem of SUM OOB GetSataInfo always showing "Configuration Type" as "AHCI" when setting "Configure SATA as" to "RAID" or "IDE".
7. Fixed inability to enter setup menu by pressing "DEL" key if Re-try Boot feature is enabled and there are no boot devices.
8. Set Descriptor Region of BIOS Region Write Access to "No".

3.0a* (02*/8/2018)

1. Implemented enhancement to address 'Spectre' variant 2 (CVE 2017-5715) security issue.
2. Updated Broadwell-EP RC 4.3.0 PLR11 release.
3. Corrected POST diagnostic signOn string.
4. Added tCCD_L Relaxation item under Memory Configuration menu.
5. Added SumBbsSupportFlag into DAT file.
6. Removed SIOM report for SMBIOS type 41 so that SIOM only reports on SMBIOS type 9.
7. Added "SMBIOS Preservation" Enabled/Disabled item for flash recovery.
8. Enhanced SMC Recovery Flash Boot Block feature.
9. Fixed inability of SUM to get COM2/SOL settings from BIOS.
10. Updated Intel Server Platform Services 3.1.3.50 for Grantley Refresh Platforms.
11. 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).
12. Fixed inability of SUM utility to get "Setup Prompt Timeout" setup item.
13. Added support for UEFI mode PXE boot via F12 hot key Net boot.
14. Changed Memory correctable threshold to 100 and enabled Cloaking for Broadwell CPU E5-26xx SKU.
15. Added support for JEDEC NVDIMM.
16. Implemented SMC Recovery Flash Boot Block feature to add the POST screen message, "The System Is Going To Reset And Then Entering To Recovery Mode Again."
17. Added Ramaxel JEDEC ID to support Ramaxel memory.
18. Fixed problem of NVDIMM setup items appearing when optimized defaults load even without NVDIMM being installed.
19. Fixed problem of SMBIOS Type4 CPU2 current speed not showing as zero when CPU2 is not installed.
20. Fixed problem of system resetting or hanging after Watch Dog function is enabled during BIOS update.
21. Fixed problem of MWAIT being disabled on BSP only.
22. Fixed inability to get correct Memory CECC DIMM location via SD5.
23. Fixed problem of system hanging at POST 0xA9 when entering setup menu while Intel P4800X uEFI driver is loaded.
24. 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.