BIOS Release Notes Form

Product Name	**X10DRT-PS**
Release Version	**3.4 SPS: 3.1.3.72**
Build Date	**5/20/2021**
Previous Version	**3.2**
Update Category	**Recommended**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Displayed "IPMI STATUS" string in IPMI setup page.** **2. Updated Grantley Refresh RC IPU2021.1 (RC 278R17) for INTEL-TA-00463 Security Advisory to address CVE-2020-12357 (7.5, High) and CVE-2020-12360 (5.6, Medium) security issues, for IPU2020.2 Intel-TA-00358 Security Advisory to address CVE-2020-0591 (6.7, Medium) and CVE-2020-0592 (3, Low) security issues, and for Intel-TA-00390 Security Advisory to address CVE-2020-8738 (7.5, High), CVE-2020-8740 (6.7, Medium), and CVE-2020-8764 (8.2, High) security issues.** **3. Updated Haswell-EP/Broadwell-EP CPU microcode from Intel-Restricted-2021-1-IPU-20210322_20211IPU Release.** **4. Updated AMI SA50072 and SA50077 security update for AHCI and WHEA modules.** **5. Prevented abnormal display when installing the AMD MI25 and setting the VGA priority to off-board.**

	6. Prioritized Disk SMART error event before display disk SMART error. **7. Patched to prevent system hang at 94 with NVidia new RTX 6000/8000.** **8. Updated 10G table for AOC-MIBE6-m1CM IB mode.**
New features	**N/A**
Fixes	**N/A**

Release Notes from Previous Release(s)

3.2 (11/20/2019)

1. Updated SINIT ACM 3.1.4 PW for Intel-SA00240 (CVE-2019-0151 CVSS 3.1: 7.5 High).
2. Updated SATA/sSATA RAID OPROM/EFI driver to VROC PreOS v6.2.0.1034.
3. Updated Broadwell-EP B0/M0/R0 CPU microcode MEF406F1_0B000038 for Intel-SA00219 (CVE-2019-0117) and Intel-SA00220 (CVE-2019-0123).

3.1c (4/27/2019)

1. Updated Intel Server Platform Services 3.1.3.72 for Grantley Refresh Platforms.
2. Updated SATA/sSATA RAID OPROM/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.
8. Displayed the driver health support pages to support LSI (Broadcom 9440-8i) driver health status.
9. Fixed malfunction of Windows Consistent Device Naming (CDN).
10. Corrected UUID with LAN chips like X710 and Mellanox.

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 (6/9/2018)

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.