BIOS Release Notes Form

Product Name	**X10DRT-P/PT/PIBF/PIBQ**
Release Version	**3.5 SPS: 3.1.3.131**
Build Date	**4/27/2022**
Previous Version	**3.4**
Update Category	**Recommended**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Refer to AMI 5.011_MayanCity_0ACFL048 to Update RC 278R48 for IPU 2022.1.** **2. Updated Haswell-EP C0,1/M0,1/R2 CPU microcode M6F306F2_00000049.** **3. Updated BIOS ACM to v3.1.5.** **4. Updated Intel Server Platform Services 3.1.3.131 for Grantley Refresh Platforms.** **5. Added UUID Enhancement for system without onboard LAN.**
New features	**None**
Fixes	**1. Checked NVMe_SUPPORT for NATIVE_NVME_ENABLE item.**

Release Notes from Previous Release(s)

3.4 (5/22/2021)

1. Displayed "IPMI STATUS" string on IPMI setup page.
2. Updated Grantley Refresh RC IPU2021.1 (RC 278R17) to address INTEL-TA-00463: CVE-2020-12357 (7.5, High) and CVE-2020-12360 (5.6, Medium) security issues.
3. Updated Haswell-EP/Broadwell-EP CPU microcode from Intel-Restricted-2021-1-IPU-20210322_20211IPU Release.

3.3 (10/24/2020)

1. Updated Haswell-EP/Broadwell-EP CPU microcode from 20201020_NDA Release.
2. Updated Grantley Refresh RC IPU2020.2 to address Intel-TA-00358: CVE-2020-0591 (6.7, Medium) and CVE-2020-0592 (3, Low), and Intel-TA-00390: CVE-2020-8738 (7.5, High), CVE-2020-8740 (6.7, Medium), and CVE-2020-8764 (8.2, High).
3. Prioritized Disk SMART error event before display of disk SMART error.

3.2 (11/19/2019)

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.
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. Forced a global reset if SPI descriptor is not write-protected after BIOS flash.
8. Implemented anti-rollback for FDT Read-Only.
9. Implemented multi-line IPMI page text and string.
10. Updated EIP393007 & EIP411789 for TPM vulnerability when resuming S3.
11. Added support for setting IPv6 Static Router1 prefix length and value in BIOS setup menu feature.
12. Displayed the driver health support pages to support LSI (Broadcom 9440-8i) driver health status.
13. Fixed malfunction of Windows Consistent Device Naming (CDN).
14. Fixed problem of BIOS always retrying boot when Re-Try Boot is Disabled.
15. Fixed malfunction of METW if many error events are triggered within a very short time.

3.1 (6/7/2018)

1. Updated CPU microcode to address 'Spectre' derivatives (CVE-2018-3639 & CVE-2018-3640) security issue.
2. Changed BIOS version to 3.1.
3. Added support for IPMI IPV6.

4. Removed unsupported memory frequency options from setup menu.
5. Updated Broadwell-EP RC 4.4.0 release.
6. Fixed problem of Afu /O command clearing SMC SMBIOS region ($SMC).
7. Fixed problem of SUM OOB GetSataInfo always showing "Configuration Type" as "AHCI" when setting "Configure SATA as" to "RAID" or "IDE".
8. Set Descriptor Region of BIOS Region Write Access to "No".

3.0a* (02*/9/2018)

1. Updated Haswell-EP C0,1/M0,1/R2 CPU microcode M6F306F2_0000003C and Broadwell-EP B0/M0/R0 CPU microcode MEF406F1_0B00002A to address 'Spectre' variant 2 (CVE 2017-5715) security issue.
2. Changed BIOS revision to 3.0a.
3. Updated Broadwell-EP RC 4.3.0 PLR11 release.
4. Updated BIOS ACM 3.1.1 PW and SINIT ACM 3.1.1 PW.
5. Added tCCD_L Relaxation item under Memory Configuration menu.
6. Added SumBbsSupportFlag into DAT file.
7. Changed Memory correctable threshold to 100 and enabled Cloaking for Broadwell CPU E5-26xx SKU.
8. Added support for JEDEC NVDIMM.
9. Implemented SMC Recovery Flash Boot Block feature.
10. Implemented dynamic update SATA re-driver settings for 1U and 2U backplane.
11. Added Ramaxel JEDEC ID to support Ramaxel memory.
12. Fixed problem of NVDIMM setup items appearing when optimized defaults load even without NVDIMM being installed.
13. Fixed problem of SMBIOS Type4 CPU2 current speed not showing as zero when CPU2 is not installed.
14. Fixed problem of system resetting or hanging after Watch Dog function is enabled during BIOS update.
15. Fixed problem of MWAIT being disabled on BSP only.
16. Fixed inability of SUM to get COM2/SOL settings from BIOS.
17. Fixed issue of BIOS setup menu having "PCI Latency Timer" option.