BIOS Release Notes Form

Product Name	**X10DRT-H(IBF)**
Release Version	**3.3 SPS: 3.1.3.72**
Build Date	**10/24/2020**
Previous Version	**3.2**
Update Category	**Recommended**
Dependencies	**None**
Important Notes	**None**
Enhancements	**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.**
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.
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. 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. Added support for setting IPv6 Static Router1 prefix length and value in BIOS setup menu feature.
11. Updated CryptoPkg 32.01 for AMI SA50066.
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 (6/9/2018)

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 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. 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).
5. Added tCCD_L Relaxation item under Memory Configuration menu.
6. Updated BIOS ACM 3.1.1 PW and SINIT ACM 3.1.1 PW.
7. Added SumBbsSupportFlag into DAT file.
8. Added "SMBIOS Preservation" Enabled/Disabled item for flash recovery.
9. Enhanced SMC Recovery Flash Boot Block feature.
10. Fixed inability of SUM to get COM2/SOL settings from BIOS.
11. Fixed inability of SUM utility to get "Setup Prompt Timeout" setup item.
12. Added support for UEFI mode PXE boot via F12 hot key Net boot.
13. Added ability of MECI (Multiple Event Count Increment) and METW (Multiple Event Time Window) to work with memory correct error and PCIe error reports.
14. Implemented Dynamic MMCFG BASE feature.
15. Added support for JEDEC NVDIMM.
16. Implemented SMC Recovery Flash Boot Block feature.
17. Fixed system hanging when plugging in an add-on card that contains non-SMC format VPD data.
18. Fixed inability to change "Processor Frequency" when setting "Boot performance mode" to "Max Efficient" by AMIBCP.
19. Fixed SUM error when running "GetCurrentBiosCfgTextFile" after BIOS setup modified by AMIBCP.
20. Fixed system hanging at POST 0xB2 when installing Mellanox MCX311a and MCX312C-XCCT.
21. Corrected MECI help string typo.
22. Fixed problem of IPMI boot command being cleared even when persistence boot has been set.
23. Fixed issue of "ChkHddInfoX64.efi -c" command failing.
24. Fixed problem of system resetting or hanging after Watch Dog function is enabled during BIOS update.
25. Fixed issue of SUM TC306 and TC317 failing in certain configuration cases.
26. Fixed issue of power button not being reported in ACPI table when set to "4 Seconds Override".
27. Fixed failure of software automation testing when riser card is plugged in.
28. Fixed issue of Super.rom not working and SUT hanging on POST 79.
29. Fixed failure of BIOS Auto Recovery.
30. Fixed problem of MWAIT being disabled on BSP only.
31. Fixed inability to get correct Memory CECC DIMM location via SD5.
32. Fixed problem of SMBIOS Type4 CPU2 current speed not showing as zero when CPU2 is not installed.
33. 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.