IPMI Firmware / BIOS Release Notes Form

Product Name	**X10DRT-L/LIBQ/LIBF**
Release Version	**3.2**
Release Date	**11/22/2019**
Previous Version	**3.1c**
Update Category	**Critical**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Changed BIOS revision to 3.2.** **2. Updated SINIT ACM 3.1.4 PW for INTEL-SA-00240 Security Advisory to address CVE-2019-0151 (7.5, High) and CVE-2019-0152 (8.2, High) security issues.** **3. Updated SATA/sSATA RAID OPROM/EFI driver to VROC PreOS v6.2.0.1034.** **4. Updated Broadwell-EP B0/M0/R0 CPU microcode MEF406F1_0B000038 for INTEL-SA-00219 Security Advisory to address CVE-2019-0117 (6.0, Medium) security issue and for INTEL-SA-00220 Security Advisory to address CVE-2019-0123 (8.2, High) and CVE-2019-0124 (8.2, High) security issues.**
New features	**N/A**
Fixes	**N/A**

Release Notes from Previous Release(s)

3.1c (05/02/2019)

1. Changed BIOS revision to 3.1c.
2. Forced a global reset if SPI descriptor is not write-protected after BIOS flash.
3. Implemented anti-rollback for FDT Read-Only.
4. Implemented multi-line IPMI page text and string.
5. Updated EIP393007 & EIP411789 for TPM vulnerability when resuming S3.
6. Updated Intel Server Platform Services 3.1.3.72 for Grantley Refresh Platforms.
7. Updated SATA/sSATA RAID OPROM/EFI driver to VROC PreOS v6.1.0.1017.
8. Updated VBIOS and VGA EFI Driver to 1.09.
9. Updated Haswell-EP/Broadwell-EP CPU microcode from SRV_P_273 for INTEL-SA-00233 Security Advisory to address CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, and CVE-2019-11091 security issues.
10. Updated valid range of IPMI setup item VLAN ID to 1-4094.
11. Added support for RFC4122 UUID format feature to set RFC4122 encoding from build time produced by IPMICFG 1.29 tool or newer.
12. Added support for setting IPv6 Static Router1 prefix length and value in BIOS setup menu feature.
13. Fixed problem of BIOS always retrying boot when Re-Try Boot is Disabled.
14. Fixed malfunction of METW if many error events are triggered within a very short time.
15. Displayed the driver health support pages to support LSI (Broadcom 9440-8i) driver health status.
16. Fixed malfunction of Windows Consistent Device Naming (CDN).

3.1 (06/06/2018)

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. Fixed failure of SMBIOS to change to default even if preserve SMBIOS setup item is set to disabled during recovery.
9. Set Descriptor Region of BIOS Region Write Access to "No".

3.0a* (02*/8/2018)

1. Changed BIOS revision to 3.0a.
2. Updated SATA RAID OPROM/EFI driver to RSTe PreOS v4.7.0.1014.
3. Updated Intel Server Platform Services 3.1.3.50 for Grantley Refresh Platforms.
4. Updated Haswell-EP C0,1/M0,1/R2 CPU microcode M6F306F2_0000003C and Broadwell-EP B0/M0/R0 CPU microcode MEF406F1_0B00002A from SRV_B_204 to address CVE-2017-5715.
5. Removed support for using Ctrl+home to trigger recovery.
6. Changed Memory correctable threshold to 100 and enabled Cloaking for Broadwell CPU E5-26xx SKU.
7. Updated BIOS ACM 3.1.1 PW and SINIT ACM 3.1.1 PW.

8. Added BBS reset function to SmcOobLoadBiosDefault().
9. Changed tCCD_L Relaxation default to 1 and changed string from Enabled to Auto.
10. Appended VPD - VB tag in VPD-W Tag(0x91) area.
11. Updated Broadwell-EP RC 4.3.0 PLR11 release.
12. Added SumBbsSupportFlag into DAT file.
13. Added support for LSI 3008/3016 HBA sensor.
14. Updated new MRC error log definition.
15. Added support for JEDEC NVDIMM.
16. Enabled OA1_SUPPORT to fix inability to modify OEM Data by AMIBCP.exe.
17. Added Intel SPI vulnerability patch for Grantley.
18. Added "SMBIOS Preservation" Enabled/Disabled item for flash recovery.
19. Displayed setup item "ACS Control" to Enable/Disable PCIe Access Control Services Extended Capability.
20. Implemented SMC Recovery Flash Boot Block feature.
21. Fixed missing Manufacturer string in SMBIOS type 17 when Ramaxel DIMM is plugged in.
22. Fixed problem of NVDIMM setup items appearing when optimized defaults load even without NVDIMM being installed.
23. Fixed problem of SMBIOS Type4 CPU2 current speed not showing as zero when CPU2 is not installed.
24. Fixed problem of system resetting or hanging after Watch Dog function is enabled during BIOS update.
25. Fixed inability to get correct Memory CECC DIMM location via SD5.
26. Fixed problem of system hanging at 79 with some NVDIMMs.