IPMI Firmware / BIOS Release Notes Form

Product Name	**X10DRFF(-C)**
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-Roll Back for FDT Read-Only and set the default setting to Disabled.
4. Implemented multi-line IPMI page text and string.
5. Updated EIP393007 and EIP411789 for TPM vulnerability for 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, and CVE-2018-12130 security issue.
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 (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. Updated Broadwell-EP RC 4.4.0 release.
4. Added support for IPMI IPV6.
5. Removed unsupported memory frequency options from setup menu.
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 (2/8/2018)

1. Updated SATA RAID OPROM/EFI driver to RSTe PreOS v4.7.0.1014.
2. Updated Intel Server Platform Services 3.1.3.50 for Grantley Refresh Platforms.
3. Updated CPU microcode SRV_B_204 for Haswell-EP C0,1/M0,1/R2 & Broadwell-EP B0/M0/R0.
4. Removed support for using Ctrl+home to trigger recovery.
5. Changed BIOS revision to 3.0a.
6. Changed Memory correctable threshold to 100 and enabled Cloaking for Broadwell CPU E5-26xx SKU.
7. Updated Broadwell-EP RC 4.3.0 PLR10 release.
8. Removed the "P1" string when Memory error occurs on UP server.
9. Corrected POST diagnostic signOn string.

10. Patched Micron Z11C DIMM to improve stability.
11. Changed tCCD_L Relaxation default to 1 and changed string from Enabled to Auto.
12. Appended VPD - VB tag in VPD-W Tag(0x91) area.
13. Updated CPU microcode SRV_P_192 for Broadwell-EP B0/M0/R0.
14. Updated new MRC error log definition.
15. Updated Intel Server Platform Services 3.1.3.38 PLR7 for Grantley Refresh Platforms.
16. Updated CPU microcode SRV_P_181 for Broadwell-EP B0/M0/R0.
17. Updated CPU microcode SRV_P_182 for Haswell-EP C0,1/M0,1/R2.
18. Added Intel SPI vulnerability patch for Grantley.
19. Updated Broadwell-EP B0/M0/R0 CPU uCode MEF406F1_0B000022.
20. Added "SMBIOS Preservation" Enabled/Disabled item for flash recovery.
21. Enhanced SMC Recovery Flash Boot Block feature.
22. Displayed setup item "ACS Control" to Enable/Disable PCIe Access Control Services Extended Capability.
23. Added BBS reset function to SmcOobLoadBiosDefault().
24. Added SumBbsSupportFlag into DAT file.
25. Added support for JEDEC NVDIMM.
26. Added support for LSI 3008/3016 HBA sensor.
27. Displayed Monitor/Mwait setup item.
28. Added ability of MECI (Multiple Event Count Increment) and METW (Multiple Event Time Window) to work with memory correct error and PCIe error reports.
29. Added VB tag to VPD data if not already present.
30. Implemented SMC Recovery Flash Boot Block feature.
31. Fixed issue of SUM TC306 and TC317 failing in certain configuration cases.
32. Fixed problem of system hanging after Watch Dog function is enabled and then BIOS is updated.
33. Fixed incorrect memory error location on UP server.
34. Fixed missing Manufacturer string in SMBIOS type 17 when Ramaxel DIMM is plugged in.
35. Fixed problem of NVDIMM setup items appearing when optimized defaults load even without NVDIMM being installed.
36. Fixed problem of system hanging on POST code 0xB2.
37. Fixed problem of system resetting or hanging after Watch Dog function is enabled during BIOS update.
38. Fixed inability to get correct Memory CECC DIMM location via SD5.
39. Fixed inability to log Patrol Scrub UCE.
40. Fixed problem of system hanging at 79 with some NVDIMMs.
41. Applied AMI EIP EIP274689 to fix some BIOS setup items not working properly with default values loaded on the CPU page.
42. Fixed issue where changes in METW or MECI values do not take effect in current boot to OS.
43. Corrected MECI help string typo.
44. Fixed system hanging at 0xA9 when the GPNV event log is full.
45. Fixed system hanging at POST 0xB2 when installing Mellanox MCX311a and MCX312C-XCCT.
46. Fixed SUM error when running "GetCurrentBiosCfgTextFile" after BIOS setup modified by AMIBCP.
47. Fixed inability to change "Processor Frequency" when setting "Boot performance mode" to "Max Efficient" by AMIBCP.
48. Fixed system hanging when plugging in an add-on card that contains non-SMC format VPD data.
49. Fixed multiple event time count not following the specifications.
50. Fixed problem of incorrect PCI slot number showing on Legacy/UEFI mode.