BIOS Release Notes Form

Product Name	**X10DRFF-C(T)G/I(T)G**
Release Version	**3.3 SPS: 3.1.3.72**
Build Date	**2/13/2021**
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).**
New features	**N/A**
Fixes	**N/A**

Release Notes from Previous Release(s)

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.
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. Added support for setting IPv6 Static Router1 prefix length and value in BIOS setup menu feature.
11. Displayed the driver health support pages to support LSI (Broadcom 9440-8i) driver health status.
12. Fixed malfunction of Windows Consistent Device Naming (CDN).
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.

3.1 (06/08/2018)

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 (2/9/2018)

1. Implemented enhancement to address 'Spectre' variant 2 (CVE 2017-5715) security patch issue.
2. Changed BIOS revision to 3.0a.
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. Removed support for using Ctrl+home to trigger recovery.
6. Added support for UEFI mode PXE boot via F12 hot key Net boot.

7. Fixed inability of SUM utility to get "Setup Prompt Timeout" setup item.
8. Updated Broadwell-EP RC 4.3.0 PLR11 release.
9. Displayed setup item "ACS Control" to Enable/Disable PCIe Access Control Services Extended Capability.
10. Updated BIOS ACM 3.1.1 PW and SINIT ACM 3.1.1 PW.
11. Added tCCD_L Relaxation item under Memory Configuration menu.
12. Added Intel SPI vulnerability patch for Grantley.
13. Added "SMBIOS Preservation" Enabled/Disabled item for flash recovery.
14. Enhanced SMC Recovery Flash Boot Block feature.
15. Added support for JEDEC NVDIMM.
16. Implemented SMC Recovery Flash Boot Block feature.
17. 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.
18. Added Ramaxel JEDEC ID to support Ramaxel memory.
19. Fixed problem of NVDIMM setup items appearing when optimized defaults load even without NVDIMM being installed.
20. Corrected POST diagnostic signOn string.
21. Fixed problem of SMBIOS Type4 CPU2 current speed not showing as zero when CPU2 is not installed.
22. Fixed problem of system resetting or hanging after Watch Dog function is enabled during BIOS update.
23. Fixed problem of MWAIT being disabled on BSP only.
24. Fixed inability to get correct Memory CECC DIMM location via SD5.