IPMI Firmware / BIOS Release Notes Form

Product Name	**X10DRL-i**
Release Version	**3.3**
Release Date	**10/24/2020**
Previous Version	**3.2**
Update Category	**Recommend**
Dependencies	**N/A**
Important Notes	**ECO #25008** **BIOS IAMGE X10DRL0.A24** **Please update BIOS with attached Flash Utility in package**
Enhancements	1. *Updated Haswell-EP/Broadwell-EP CPU microcode from 20201020_NDA Release.* 2. *Update Broadwell-EP RC IPU2020.2 release.* 3. *Update AMI SA50072, SA50077 security update for AHCI and WHEA modules.* 4. *To avoid abnormal display when installing the AMD MI25 and setting the VGA priority to off-board.* 5. *Prioritize Disk SMART error event before display disk SMART error.* 6. *Patch to avoid system hang at 94 with NVidia new RTX 6000/8000*
New features	*N/A*
Fixes	*N/A*

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 IntelSA00220 (CVE-2019-0123).*
4. *Updated AMI EIP453732, EIP470365, EIP451538, and CryptoPkg 32.01 for AMI SA50066.*

3.1c (5/2/2019)

5. *Changed BIOS revision to 3.1c.*
6. *Forced a global reset if SPI descriptor is not write protected after BIOS flash.*
7. *Implemented anti-rollback for FDT Read-Only.*
8. *Implemented multi-line IPMI page text and string.*
9. *Updated EIP393007 & EIP411789 for TPM vulnerability when resuming S3.*
10. *Updated Intel Server Platform Services 3.1.3.72 for Grantley Refresh Platforms.*
11. *Updated SATA/sSATA RAID OPROM/EFI driver to VROC PreOS v6.1.0.1017.*
12. *Updated VBIOS and VGA EFI Driver to 1.09.*
13. *Updated Haswell-EP/Broadwell-EP CPU microcode from SRV_P_273 for INTEL-SA-00233 Security Advisory.*
14. *Updated valid range of IPMI setup item VLAN ID to 1-4094.*
15. *Added support for RFC4122 UUID format feature to set RFC4122 encoding from build time produced by IPMICFG 1.29 tool or newer.*
16. *Added support for setting IPv6 Static Router1 prefix length and value in BIOS setup menu feature.*
17. *Fixed problem of BIOS always retrying boot when Re-Try Boot is Disabled.*
18. *Fixed malfunction of METW if many error events are triggered within a very short time.*
19. *Displayed the driver health support pages to support LSI (Broadcom 9440-8i) driver health status.*
20. *Fixed malfunction of Windows Consistent Device Naming (CDN).*
1. *updated.*
2. *Fixed missing Manufacturer string in SMBIOS type 17 when Ramaxel DIMM is plugged in.*
3. *Fixed problem of NVDIMM setup items appearing when optimized defaults load even without*

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 RSTe PreOS v5.5.0.1028 (RSTe 5.5.0.2015).
3. Updated VBIOS and VGA EFI Driver to 1.09.
4. Updated Haswell-EP/Broadwell-EP CPU microcode from SRV_P_268.
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. Updated SATA/sSATA RAID OPROM/EFI driver to VROC PreOS v6.1.0.1017.
13. Displayed the driver health support pages to support LSI (Broadcom 9440-8i) driver health status.
14. Fixed malfunction of Windows Consistent Device Naming (CDN).
15. Fixed problem of BIOS always retrying boot when Re-Try Boot is Disabled.
16. 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 IPMI IPV6 support.
4. Removed unsupported memory frequency options from setup menu.
5. Updated Broadwell-EP RC 4.4.0 release
6. Fixed Afu /O command will clear SMC SMBIOS region ($SMC).
7. Fixed SUM OOB GetSataInfo always shows "Configuration Type" as "AHCI" when setting "Configure SATA as" to "RAID" or "IDE".
8. Fixed based on Intel recommended settings to set Descriptor Region of BIOS Region Write Access to "No".

3.0a (2/9/2018)

1. Updated CPU microcode to address 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. Added Ramaxel JEDEC ID to support Ramaxel memory.
11. Fixed problem of NVDIMM setup items appearing when optimized defaults load even without NVDIMM being installed.
12. Fixed problem of SMBIOS Type4 CPU2 current speed not showing as zero when CPU2 is not installed.
13. Fixed problem of system resetting or hanging after Watch Dog function is enabled during BIOS update.

14. Fixed problem of MWAIT being disabled on BSP only