BIOS Release Notes Form

Product Name	**X11DSN-TS(Q)**
Release Version	**3.8b SPS: 4.1.04.901**
Build Date	**01/06/2023**
Previous Version	**3.6**
Update Category	**Recommended**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Changed BIOS revision to 3.8b.** **2. Updated AMI label 5.14_PurleyCrb_0ACLA058 for RC0626.P01 IPU 2023.1.** **a) For INTEL-SA-00717 Security Advisory to address CVE-2022-32231 (7.5, High) / CVE-2022-26343 (8.2, High) security issues.** **3. Updated token RC_VERSION_VALUE setting to 626.P01.** **4. Updated Cascade Lake-SP CPU PV microcode for IPU 2023.1.**
New features	**None**
Fixes	**None**

Release Notes from Previous Release(s)

3.6 (1/12/2022)

1. *Changed BIOS revision to 3.6.*
2. *Updated SATA/sSATA EFI driver to VROC PreOS v7.7.0.1054.*
3. *Updated AEP uEFI driver to 1.0.0.3531 for IPU2021.2.*
4. *Updated AMI label 5.14_PurleyCrb_0ACLA054 for RC0616.D08 2021.2 IPU.*
5. *Updated Intel Server Platform Services for Purley Refresh Server Platforms IPU2021.2 HF1 4.1.4.654.*
6. *Updated BIOS ACM 1.7.51, SINIT ACM 1.7.51 PW*
7. *Updated Skylake-SP/Cascade Lake-SP CPU PV microcode, Skylake-SP H0/M0/U0 stepping CPU PV microcode, MB750654_02006C0A, Cascade Lake-SP B0 stepping CPU PV microcode MBF50656_0400320A, Cascade Lake-SP B1 stepping CPU PV microcode MBF50657_0500320A.*

3.4 (11/4/2020)

1. *Updated AMI EIP563137 to fix failure of some BIOS items (like boot mode item) to load default with some configurations (like with Micron M.2 or HGST SATA M.2).*
2. *Fixed problem of EFI version of PassMark MemTest86 hanging when SMCI Redfish Host Interface is not supported in IPMI firmware.*
3. *Fixed failure of "UEFI Compliant - Boot from iSCSI peripheral" in UEFI SCT test.*
4. *Fixed problem of system hanging during BIOS flash if Watch Dog function is enabled.*
5. *Fixed inability of 6240R and some refresh 4 serial CPU frequencies to reach maximum when enabling Mwait.*
6. *Corrected BMC firmware revision in BIOS Setup.*
7. *Fixed inconsistency of X-AMI ID of Setup Item "Refresh Watermarks".*
8. *Enhanced SMCI HDD Security feature.*
9. *Added force next boot to UEFI Shell via IPMI support.*
10. *Added function to move all LANs to the top of boot priority when IPMI forces PXE.*
11. *Added inband flash status event log to IPMI MEL.*
12. *Corrected "Station MAC Address" display order when "Configuration Address Source" is set to "Static".*
13. *Added PPR success result SEL and set duplicated PPR SELs to be filtered out if the location is same.*
14. *Added VMWare PMem for VMWware Certification Allowance for PMEM Optane Memory, displayed Config TDP control item, and added help string for HttpBoot item "Input the description".*
15. *Updated 5.14_PurleyCrb_0ACLA052 for RC update and 2020.2 IPU PV to address Intel-TA-00358: CVE-2020-0587 (6.7, Medium), CVE-2020-0591 (6.7, Medium), CVE-2020-0592 (3, Low), and Intel-TA-00390: CVE-2020-0593 (4.7, Medium), CVE-2020-8738 (7.5, High), CVE-2020-8739 (4.6, Medium), CVE-2020-8740 (6.7, Medium), and CVE-2020-8764 (8.7 High) security issues.*
16. *Updated BIOS ACM 1.7.41 and SINIT ACM 1.7.49 PW for IPU2020.2 to address Intel-TA-00358: CVE-2020-0588 (3.8, Low) and CVE-2020-0590. (7.7, High) security issues.*
17. *Updated SPS 4.1.4.423 to address Intel-TA-00391: CVE-2020-8755 (4.6, Medium) and CVE-2020-8705 (7.1, High) security issues.*
18. *Updated Skylake-SP/Cascade Lake-SP CPU PV microcode from 20200918_NDA Release to address Intel-TA-00381: CVE-2020-8696 (2.5, Low) security issue, MD_Clear Errata, MOB Speedpath, and IRR Restore with RS Throttle (ITR #2).*
19. *Updated SATA/sSATA RAID OPROM/EFI driver to VROC PreOS v6.3.0.1005 PV.*

3.3 (02/19/2020)

1. Updated BIOS ACM to 1.7.40 and SINIT ACM to 1.7.48 PW.
2. Changed patrol scrub from uncorrectable to correctable error as a CLX28 workaround.
3. Added support for SMC HDD Security password erase and reset.
4. Updated Skylake-SP/Cascade Lake-SP CPU microcode for Intel-SA-00329 (CVE2020-0548 2.8 Low, CVE2020-0549 6.5 Medium), Intel-SA-00288 (CVE2019-11157 5.3 Medium), and Intel-SA-00317 (CVE2019-14607 7.9 High).
5. Updated AMI label 5.14_PurleyCrb_0ACLA050 beta for IPU2020.1 PV.
6. Updated SPS_E5_04.01.04.381 from IPU 2020.1 PV.
7. Updated BIOS menu with "tRFC Performance Enable", "Panic and High Watermark", and "Balanced Profile" options.
8. Fixed the value of BIOS Control Register bit 9 during Intel Self-Test 7 v111 SPI/DCh BIOS_CNTL.
9. Enabled UPI correctable error logging in BIOS event log and IPMI SEL.
10. Removed IMC interleave from extreme performance mode if IMC interleave is not AUTO.
11. Enabled HTTP/HTTPS booting even when USB UNDI module is enabled.

3.2 (10/22/2019)

1. Updated AMI label 5.14_PurleyCrb_0ACLA049_BETA for BKC WW36 RC595.D04 for AMI security update SA50072, IPU 2019.2 INTEL-SA-00280 Security Advisory to address CVE-2019-11136 (7.5, High) and CVE-2019-11137 (7.5, High) security issues.
2. Updated SINIT ACM 1.7.3 PW from BKC WW36 IPU 2019.2 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 SPS_E5_04.01.04.339.0 from BKC WW36 IPU 2019for INTEL-SA-00241 Security Advisory to address CVE-2019-11090 (6.8, Medium), CVE-2019-11088 (7.5, High), CVE-2019-0165 (4.4, Medium), CVE-2019-0166(5.9, Medium), CVE-2019-0168 (4.6, Medium), CVE-2019-0169 (9.6, Critical), CVE-2019-11086 (3.5, Low), CVE-2019-11087 (6.4, Medium), CVE-2019-11101 (4.4, Medium), CVE-2019-11100 (6.1, Medium), CVE-2019-11102 (4.1, Medium), CVE-2019-11103 (7.3, High), CVE-2019-11104 (7.3, High), CVE-2019-11105 (7.9, High), CVE-2019-11106 (4.4, Medium), CVE-2019-11107 (5.3, Medium), CVE-2019-11108 (2.3, Low), CVE-2019-11110 (4.1, Medium), CVE-2019-11097 (7.3, High), CVE-2019-0131 (7.1, High), CVE-2019-11109 (4.4, Medium), CVE-2019-11131 (7.5, High), CVE-2019-11132 (8.4, High), and CVE-2019-11147 (8.2, High) security issues.
4. Updated Skylake-SP/Cascade Lake-SP CPU microcode from Intel-Generic-Microcode-20191004_NDA for INTEL-SA-00271 Security Advisory to address CVE-2019-11139 (5.8, Medium) security issue.
5. Fixed ability to see memory correctable error event during MRC when use a single bit bad DIMM.
6. Changed "Secure Boot Mode" to ReadOnly attribute.
7. Displayed Setup item "ARI Support".
8. Prevented SDDC and ADDDC from graying out when Run Sure is enabled.
9. Added support for firmware version information.
10. Fixed mismatch of Secure Boot value.
11. Fixed problem of setup pages disappearing after ReadyToBoot.
12. Set software threshold for non-fatal MCE error with yellow status to enabled as default.
13. Enhanced support for Intel Speed Select.
14. Implemented dynamic change for Secure Boot Mode default value.
15. Added support for keeping Linux MOK keys database.
16. Added Redfish/SUM Secure Boot feature to update OOB for secure boot and reserve Key.
17. Updated VBIOS and VGA EFI Driver to 1.10.

18. Added recommended AEP DIMM firmware version.
19. Enhanced F12 hot key PXE boot feature.
20. Updated SATA/sSATA RAID OPROM/EFI driver to VROC PreOS v6.2.0.1034.
21. Disabled ADDDC/SDDC and set PPR as hPPR.
22. Updated RC595.D04 hot fix. 1. Added Enhanced PPR function.
23. Removed PXE option for "OnBoard LanX Option ROM" when "Boot mode select" is UEFI.
24. Fixed inability of InBand Update BIOS in Linux OS to preserve Linux secureboot keys.
25. Fixed inability to identify duplicate boot options with more than one of the same M.2 AHCI interface devices.
26. Fixed problem of boot time increasing by more than two minutes per boot after running stress over hundreds of cycles.
27. Changed OOB download and Upload Bios Configuration sequence.
28. Fixed failure of the default boot order of UEFI groups to sync when "Boot mode" is under UEFI mode.
29. Fixed problem of key details showing "Security Violation" after loading Factory secure boot keys.
30. Masked AP Mwait instruction if needed.
31. Removed SNC override when set to extreme performance mode.
32. Removed Intel Virtualization Technology override when set to extreme performance (in extreme performance mode support only).

3.1 (5/2/2019)

1. Updated Skylake-SP/Cascade Lake-SP CPU microcode.
2. Updated Intel BKCWW16 2019 PV PLR1.
3. Updated SPS_E5_04.01.04.296.0 from BKC WW16 2019.
4. Updated EIP467272 for AMI SA50069, SA50070.
5. Set SDDC Plus One or SDDC to disabled by default.
6. Updated SATA/sSATA RAID OPROM/EFI driver to VROC PreOS v6.1.0.1017.
7. Set ADDDC Sparing to enabled by default.
8. Set BMC MAC address to UUID for system without onboard LAN1 or with onboard LAN1 disabled.
9. Set PCIe correctable and uncorrectable (non-fatal) error report to disabled by default.
10. Set RFC4122 encoding to only be enabled for build time produced by IPMI 1.29 or newer.
11. Disabled unused SPS ME "CUPS IIO" and "Volumetric Airflow" sensor.
12. Updated valid range of IPMI setup item VLAN ID to 1-4094.
13. Added driver health warning message.
14. Hid Driver Health page for SUM.
15. Set NVDIMM ADR timeout to 600us.
16. Enhanced the solution for the error/warning message from dmidecode after a modification by AMIDE.
17. Enhanced BIOS setup menu to auto-switch the Option ROM's value and hide the unexpected value when boot mode changes.
18. Enhanced BIOS setup menu to switch the boot mode value and Option ROM's values when CSM support is disabled and applied this to enabled secure boot mode case.
19. Fixed inability to change IPv6 address or IPv6 Router1 IP address.
20. Corrected DMI table type 41 number when installing different types of SIOM add-on card.
21. Fixed problem of setup item "Quiet Boot" staying enabled after flashing BIOS with "Quiet Boot" disabled.
22. Fixed problem of the system equipped with dTPM 2.0 hanging up at POST code 0x90 when disabling dTPM 2.0 by SUM TPM OOB command "--disable_dtpm".

23. Corrected TPM RSD ChangeTPMState behavior to control TPM 1.2/2.0 state instead of "Security Device Support".
24. Fixed problem of TPM 2.0 device disappearing when disabling "RSD PSME ChangeTPMState API" and then enabling TPM 2.0 state.
25. Modified UEFI network description to IPv4/IPv6 to follow Industry Standard.
26. Fixed inability to log SERR event for ASC-29320LPE.
27. Fixed problems of system hanging up at POST code 0x92 and rebooting endlessly during POST and inability to get PPIN under OS (DOS/EFI shell/Windows/Linux).
28. Fixed failure to log memory UCE event due to incorrect flag.
29. Fixed inability of "Network Stack"-related items to get/change via SUM OOB method.
30. Fixed incorrect display of the TDP of Intel Speed Select table.
31. Patched problem of incorrect memory power being reported in PTU.
32. Applied workaround for inability of SUM to get full setting of IODC setup item.
33. Temporarily fixed error for SKX (CLX) 4114 CPU memory training with Micron (18ASF2G72PDZ-2G6E1) RDIMM.
34. Fixed loss of all LAN items when boot mode changes from Dual mode to UEFI mode.

3.0a (1/29/2019)

1. Added support for Purley Refresh platform.
2. Updated AMI label 5.14_PurleyCrb_0ACLA040.1_BETA, BKC WW02 2019.
3. Updated SINIT ACM 1.7.1 PW from BKC WW02 2019.
4. Updated SATA RAID OPROM/EFI driver to RSTe PreOS v6.0.0.1024.
5. Set PCIe correctable and uncorrectable (non-fatal) error report to disabled by default.
6. Added support for RFC4122 UUID format feature to set RFC4122 encoding from build time produced by IPMICFG 1.29 tool or newer.
7. Set NVDIMM ADR timeout to 600us.
8. Fixed problem of setup item "Quiet Boot" staying enabled after flashing BIOS with "Quiet Boot" disabled.