BIOS Release Notes Form

Product Name	**X11DPH-I/T/T(Q)**
Release Version	**3.8b SPS: 4.1.04.901**
Build Date	**01/06/2023**
Previous Version	**3.8a**
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)

3.8a (10/28/2022)

1. *Updated the AMI label 5.14_PurleyCrb_0ACLA057 for RC0623.D09 2022.3 IPU.*
   a) *For INTEL-TA-00610 Security Advisory to address CVE-2022-26845 (8.7 High), CVE-2022-27497(8.6 High), CVE-2022-29893 (8.1 High), CVE-2021-33159 (7.4 High), CVE-2022-29466(7.3 High), and CVE-2022-29515(6.0 Medium) security issues.*
   b) *For INTEL-TA-00688 Security Advisory to address CVE-2022-26006 (8.2 High) and CVE-2022-21198(7.9 High) security issues.*
2. *Updated token RC_VERSION_VALUE setting to 623.D09.*
   Updated token PRICESSO_0_UCODE_VERSION setting to 02006E05.
   Updated token FW_SPS_VERSION setting to 4.1.4.804.
3. *Updated Intel DCPM UEFI driver to 1.0.0.3536.*
4. *Updated Skylake-SP/Cascade Lake-SP CPU PC microcode for IPU 2022.2.*
   a) *For INTEL-SA-00601 Security Advisory to address CVE-2021-0154(8.2, High), CVE-2021-0153(8.2, High), CVE-2021-33123(8.2, High), CVE-2021-0190(8.2, High), CVE-2021-33122(7.9, High), CVE-2021-33060(7.8, High), CVE-2021-0189(7.5, High), CVE-2021-33124(7.5, High), CVE-2021-33103(7.5, High), CVE-2021-0159(7.4, High), CVE-2021-0188(5.3, Medium), and CVE-2021-0155(4.4, Medium) security issues.*
   b) *For INTEL-SA-00615 Security Advisory to address CVE-2022-21123(6.1, Medium), CVE-2022-21127(5.6, Medium), CVE-2022-21125(5.5, Medium), and CVE-2022-21166(5.5, Medium) security issues.*
   c) *For INTEL-SA-00616 Security Advisory to address CVE-2021-21131(3.3, Low) and CVE-2021-21136(2.7, Low) security issues.*
5. *Fixed incorrectly shown DIMM location in event log page.*
6. *Modified String naming from SMCI to Supermicro.*
7. *Removed "Vendor Keys" in security page.*
8. *[SMIHandlerSecurityFix]*
   a) *Refined SMM buffer validation in SmmSmbiosELogInitFuncs.*
   b) *Allocated runtime buffer to trigger ELog SMI in DxeSmmRedirFuncs.*
9. *Updated BIOS ACM 1.7.54, SINIT ACM 1.7.55 PW for IPU2022.1 to address Intel-TA-00161: CVE-2021-0159 (7.8 High) CVE-2021-33123 (8.2 High) and CVE-2021-33124 (7.5 High).*
10. *Updated VROC SATA/sSATA EFI driver to VROC PreOS v7.8.0.1012 to address:*
    a) *Data Loss Exposure Due to RAID 5 TRIM Support (Document #737276)*
    b) *INTEL-TA-00692. CVE-2022-29919(7.8 High), CVE-2022-30338(6.7 Medium), CVE-2022-29508(6.3 Medium), and CVE-2022-25976(5.5 Medium)*
11. *Modified the allocated buffer from EfiBootServicesData to EfiRuntimeServicesData.*
12. *Disabled MROM1 device since product doesn't use Intel IE function.*
13. *Enabled IScsi_SUPPORT on Purley generation.*

3.6 (2/8/2022)

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 to 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.*
8. *Fixed system hang at POST code 0xAF with latest BMC after run SUM test case 113 problem.*

9. Fixed CVE-2020-8673, which is not enabled with FPGA support (X11DPH/X11DPU-ZE only).

3.5 (5/19/2021)

1. Updated RC 612.D02 for INTEL-SA-00463 Security Advisory to address CVE-2020-12357 (7.5, High), CVE-2020-8670 (7.5, High), CVE-2020-8700 (7.5, High), CVE-2020-12359 (7.1, High), CVE-2020-12358 (6.7, Medium), CVE-2020-12360 (5.6, Medium), CVE-2020-24486 (5.5, Medium), and CVE-2020-0589 (3.8, Low) security issues.
2. Updated BIOS ACM 1.7.43, SINIT ACM 1.7.4A PW for INTEL-SA-00463 Security Advisory to address CVE-2020-12357 (7.5, High), CVE-2020-8670 (7.5, High), CVE-2020-8700 (7.5, High), CVE-2020-12359 (7.1, High), CVE-2020-12358 (6.7, Medium), CVE-2020-12360 (5.6, Medium), CVE-2020-24486 (5.5, Medium), and CVE-2020-0589 (3.8, Low) security issues.
3. Updated Skylake-SP/Cascade Lake-SP CPU PV microcode for INTEL-SA-00464 Security Advisory to address CVE-2020-24511 (5.6, Medium), and CVE-2020-24512 (2.8, Low) security issues.
4. Updated Intel Server Platform Services for Purley Refresh Server Platforms 4.1.4.505.
5. Updated AEP FW to FW_1.2.0.5446, uEFI driver to 3515 for IPU2021.1.
6. Added sync IPv6 status detection rule with BMC to make sure the IPv6 status is the same in BIOS and BMC web.

3.4a (1/7/2021)

1. Enabled system to boot into PXE with DVD installed.

3.4 (11/3/2020)

1. 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.
2. 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.
3. 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.
4. 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).
5. Updated SATA/sSATA RAID OPROM/EFI driver to VROC PreOS v6.3.0.1005 PV.
6. Enhanced SMCI HDD Security feature.
7. Added force next boot to UEFI Shell via IPMI support.
8. Added function to move all LANs to the top of boot priority when IPMI forces PXE.
9. Added inband flash status event log to IPMI MEL.
10. Corrected "Station MAC Address" display order when "Configuration Address Source" is set to "Static".
11. Added PPR success result SEL and set duplicated PPR SELs to be filtered out if the location is same.
12. 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".
13. 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).

14. Fixed problem of EFI version of PassMark MemTest86 hanging when SMCI Redfish Host Interface is not supported in IPMI firmware.
15. Fixed failure of "UEFI Compliant - Boot from iSCSI peripheral" in UEFI SCT test.
16. Fixed problem of system hanging during BIOS flash if Watch Dog function is enabled.
17. Fixed inability of 6240R and some refresh 4 serial CPU frequencies to reach maximum when enabling Mwait.
18. Corrected BMC firmware revision in BIOS Setup.
19. Fixed problem of system hanging at 0xB2 with some NVMe devices.
20. Fixed problem of system hanging at POST code 0xA0 or 0xA2 when using unsupported security NVMe device and installing Hyper-V with Windows 2019.

3.3 (02/24/2020)

1. Updated AMI label 5.14_PurleyCrb_0ACLA050 beta for IPU2020.1 PV.
2. Updated SPS_E5_04.01.04.381 from IPU 2020.1 PV.
3. Updated BIOS ACM 1.7.40 and SINIT ACM 1.7.48 PW.
4. Enabled saving memory CE location into PPR variable at runtime even if memory correctable error reporting is disabled.
5. Added sighting CLX28 workaround and downgraded patrol scrub UC to CE.
6. Added setup item "HDD password prompt Control" to control "Hard-Drive Password Check" for enabling/disabling HDD password prompt window during POST.
7. Updated Skylake-SP/Cascade Lake-SP CPU microcode for Intel-SA-00329 (CVE2020-0548 2.8 Low and CVE2020-0549 6.5 Medium), Intel-SA-00288 (CVE2019-11157 5.3 Medium), and Intel-SA-00317 (CVE2019-14607 7.9 High).
8. Added SMC HDD Security feature.
9. Fixed mismatch of Secure Boot Mode value.
10. Removed requirement to use Admin password for erasing TCG device.
11. Fixed problem of two CentOS boot items occurring in boot order if CentOS is installed in RAID 1 system.

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 2019 for 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. Changed "Secure Boot Mode" to ReadOnly attribute.
6. Displayed Setup item "ARI Support".

7. Prevented SDDC and ADDDC from graying out when Run Sure is enabled.
8. Added support for firmware version information.
9. Fixed mismatch of Secure Boot value.
10. Fixed problem of setup pages disappearing after ReadyToBoot.
11. Enhanced support for Intel Speed Select.
12. Implemented dynamic change for Secure Boot Mode default value.
13. Added setup item to control 16Gb based Single Die Package DIMM tRFC optimization.
14. Added support for keeping Linux MOK keys database.
15. Added Redfish/SUM Secure Boot feature to update OOB for secure boot and reserve Key.
16. Updated VBIOS and VGA EFI Driver to 1.10.
17. Added recommended AEP DIMM firmware version.
18. Enhanced F12 hot key PXE boot feature.
19. Updated SATA/sSATA RAID OPROM/EFI driver to VROC PreOS v6.2.0.1034.
20. Disabled ADDDC/SDDC and set PPR as hPPR.
21. Updated RC595.D04 hot fix.
22. Added Enhanced PPR function.
23. Removed PXE option for "OnBoard LanX Option ROM" when "Boot mode select" is UEFI.
24. Corrected display of the IPMI AUX revision.
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. Fixed inability to identify duplicate NVMe boot options with more than one of the same NVMe drives on an add-on card.
28. Changed OOB download and Upload Bios Configuration sequence.
29. Fixed failure of the default boot order of UEFI groups to sync when "Boot mode" is under UEFI mode.
30. Fixed problem of key details showing "Security Violation" after loading Factory secure boot keys.
31. Masked AP Mwait instruction if needed.

3.1 (5/22/2019)

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. Displayed 3rd IPMI version in BIOS setup.
6. Set SDDC Plus One or SDDC to disabled by default.
7. Updated SATA/sSATA RAID OPROM/EFI driver to VROC PreOS v6.1.0.1017.
8. Changed OPROM settings to EFI for OEM BIOS that only changes the boot mode to UEFI without other changes.
9. Set ADDDC Sparing to enabled by default.
10. Fixed inability to change IPv6 address or IPv6 Router1 IP address.
11. Fixed problem of PCH uplink dropping during ONOFF test.

3.0c (03/28/2019)

1. Updated Intel BKCWW10 2019 PV MR3.
2. Updated SPS_E5_04.01.04.256.0 from BKC WW08 2019.
3. Updated SINIT ACM 1.7.2 PW from BKC WW06 2019.

4. Updated Skylake-SP/Cascade Lake-SP CPU microcode from SRV_P_272.
5. Hid Driver Health page for SUM.
6. Reduced redundant reboot for offboard VGA switching.
7. Enhanced the solution for the error/warning message from dmidecode after a modification by AMIDE.
8. Enhanced BIOS setup menu to auto-switch the Option ROM's value and hide the unexpected value when boot mode changes.
9. 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.
10. 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".
11. Corrected TPM RSD ChangeTPMState behavior to control TPM 1.2/2.0 state instead of "Security Device Support".
12. Fixed problem of TPM 2.0 device disappearing when disabling "RSD PSME ChangeTPMState API" and then enabling TPM 2.0 state.
13. Modified UEFI network description to IPv4/IPv6 to follow Industry Standard.
14. 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).
15. Fixed failure to log memory UCE event due to incorrect flag.
16. Fixed inability of "Network Stack"-related items to get/change via SUM OOB method.
17. Fixed incorrect display of the TDP of Intel Speed Select table.
18. Patched problem of incorrect memory power being reported in PTU.
19. Applied workaround for inability of SUM to get full setting of IODC setup item.
20. Temporarily fixed error for SKX (CLX) 4114 CPU memory training with Micron (18ASF2G72PDZ-2G6E1) RDIMM.
21. Fixed failure to boot into VMware OS when set to Maximum Performance even if Monitor/MWAIT is enabled.

3.0a (1/24/2019)

1. Added support for Purley Refresh platform.
2. Updated SATA RAID OPROM/EFI driver to RSTe PreOS v6.0.0.1024.
3. Added 2933 to memory POR.
4. Set PCIe correctable and uncorrectable (non-fatal) error report to disabled by default.
5. Added support for RFC4122 UUID format feature to set RFC4122 encoding from build time produced by IPMICFG 1.29 tool or newer.
6. Updated CPU microcode SRV_P_262 for Skylake-SP H0/M0/U0 CPUs.
7. Disabled unused SPS ME "CUPS IIO" and "Volumetric Airflow" sensor.
8. Added support for Linux built-in utility efibootmgr.
9. Fixed problem of setup item "Quiet Boot" staying enabled after flashing BIOS with "Quiet Boot" disabled.
10. Corrected standard NVDIMM ADR time.
11. Fixed incorrect PBF high frequency core number when Hyper-Threading is disabled.
12. Added workaround for failure of BIOS flash with 156 bytes PubKey (Error: "Secure Flash Rom Verify Fail").

2.1 (6/15/2018)

1. Updated CPU microcode to address 'Spectre' derivatives (CVE-2018-3639 & CVE-2018-3640) security issue.

2. Updated BIOS ACM 1.3.7 and SINIT ACM 1.3.4.
3. Updated 5.12_PurleyCrb_0ACFD087Beta for Purley Skylake platform PLR6, BKC 2018 WW14.
4. Updated SATA RAID OPROM/EFI driver to RSTe PreOS v5.4.0.1039.
5. Corrected BIOS/ME downgrade check for SPS 4.0.4.340.
6. Added SMC_BUS_MASTER_EN token for enabling SMC Bus Master or AMI DMA AMI BME DMA Mitigation in setup.
7. Updated Giga LAN EFI driver 8.3.0.4 (IBA 23.1).
8. Added support for UEFI mode PXE boot of F12 hot key Net boot.
9. Added support for RFC3021.
10. Corrected default setting for Enable SmcBusMasterEn setup item.
11. Checked PCH SKU for QAT enabled board.
12. Fixed problem of system hanging when installing Linux OS after COM1 & COM2 IO/IRQ exchange.
13. Fixed problem of Ctrl + Alt + Del causing system to hang after flashing BIOS.
14. Fixed problem of DMI being lost if DMI is changed and then UpdateBios is run.
15. Fixed problem of SUM GetSataInfo showing incorrect "Configuration Type" when setting "Configure sSATA as" to "AHCI" or "RAID" on sSATA controller.
16. Fixed failure of WDT function.

2.0b (2/27/2018)

1. Implemented enhancement to address 'Spectre' variant 2 (CVE 2017-5715) security patch issue.
2. Added setup item "SmcBusMasterEn" for enabling Parent bridge of the devices in the gSmcPciForceEnableBusMasterList.
3. Updated Purley RC 151.R03.
4. Updated BIOS ACM 1.3.5 and SINIT ACM 1.3.3.
5. Changed PCH uplink CTLE/VGA/TSM SI setting to [4,10,32].
6. Changed RC default setting to upgrade POST Memory correctable error to uncorrectable error and map out the channel.
7. Fixed problem of DMI being cleared when running SUM LoadDefaultBiosCfg.
8. Disabled CPU2 IIO PCIe root port ACPI hot plug function.
9. Fixed issue with IPMI force boot.
10. Fixed problem of SMC skipping first boot option in UEFI mode when retrying boot.
11. Fixed inability to reset the system under DOS by pressing "Ctrl-Alt-Del" on USB keyboard when "Port 60/64 Emulation" is disabled.
12. Fixed inability of some CPUs to display correct microcode revision under BIOS setup menu.
13. Fixed problem of system hanging during BIOS flashing if Watch Dog function is enabled.
14. Fixed problem of the system not logging memory errors upon injection without rebooting.
15. Fixed inability of BIOS to boot into OS with Intel P3608 PCIe NVMe drive installed.

2.0a (12/16/2017)

1. Updated CPU microcode SRV_P_217 for Skylake-EP H0/M0/U0 stepping CPUs.
2. Fixed problem of system hanging during BIOS flashing if Watch Dog function is enabled.
3. Fixed problem of the system not logging memory errors upon injection without rebooting.
4. Fixed inability to boot into OS that's installed on Intel P3608 PCIe NVMe drive.

2.0 (11/30/2017)

1. Updated SATA RAID OPROM/EFI driver to RSTe PreOS v5.3.0.1052.
2. Updated the onboard X722 Lan NVM to 722PAD1C.

3. Reduced the boot time caused by IPv4/IPv6 polling.
4. Updated BIOS ACM 1.3.4.
5. Added support for AOC-SLG3-2M2 rev. 1.00 AOC cards (M.2 Riser Card).
6. Updated SPS 4.00.04.294 PLR 3.1 PV version.
7. Updated CPU microcode SRV_P_214 for Skylake-EP H0/M0/U0 stepping CPUs.
8. Updated 5.12_PurleyCrb_0ACFD084_BETA for Purley Skylake platform PLR 3.1.
9. Fixed failure of the IIO Root port PCIe manual bifurcation.
10. Fixed problem of system rebooting endlessly when equipping dTPM module.
11. Fixed problem of DMI being cleared when running SUM LoadDefaultBiosCfg.