BIOS Release Notes Form

Product Name	**X11DPT-B(H)**
Release Version	**3.8 SPS: 4.1.04.804**
Release Date	**8/24/2022**
Previous Version	**3.6**
Update Category	**Recommended**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Updated AMI label 5.14_PurleyCrb_0ACLA056 for RC0622.D07 2022.2 IPU.** **2. Updated Skylake-SP/Cascade Lake-SP CPU microcode for IPU 2022.2.** **3. Updated AEP uEFI driver to 01.00.00.3534 for IPU2022.2.** **4. Modified the allocated buffer from EfiBootServicesData to EfiRuntimeServicesData.** **5. Modified BIOS setup string from SMCI to Supermicro.** **6. Updated VROC SATA/sSATA EFI driver to VROC PreOS v7.8.0.1012 to address two issues: 1. Data Loss Exposure Due to RAID 5 TRIM support and 2. INTEL-TA-00692 (CVE-2022-29919(7.8 High), CVE-2022-30338(6.7 Medium), CVE-2022-29508(6.3 Medium), CVE-2022-25976(5.5 Medium)).** **7. Updated DBX file to fix Secure Boot Bypass issue.**
New features	**N/A**
Fixes	**1. Fixed the DIMM location in the event log page.**

Release Notes from Previous Release(s)

3.6 (12/31/2021)

1. Updated AMI label 5.14_PurleyCrb_0ACLA054.01 for RC0616.D08 2021.2 IPU.
2. Updated Intel Server Platform Services for Purley Refresh Server Platforms IPU2021.2 HF1 4.1.4.654.
3. Updated the SATA/sSATA EFI driver to VROC PreOS v7.7.0.1054.
4. Fixed the memory frequency in the BIOS menu with 2133 and 2933 DIMMs installed.
5. Fixed non-ASCII characters in the OEM ID and the OEM TABLE ID in the ACPI Table WSMT (Windows SMM Security Mitigations Table).
6. Fixed the "Configuration Address Source" to show "DHCP" in the setup menu.

3.5 (5/15/2021)

1. Updated RC 612.D02 and IPU 2021.1 PV 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 Skylake-SP/Cascade Lake-SP CPU PV microcode for IPU2021.1 Intel-TA-00464: CVE-2020-24511 (5.6, Medium) and other security issues.
3. Enabled system to boot into PXE with DVD installed.
4. Updated SATA/sSATA EFI driver to VROC PreOS v7.5.0.1152 PV.
5. Added support for IPMI UEFI PXE boot to all LAN ports feature.
6. Added support for IPv6 HTTP Boot function.
7. Updated Intel Server Platform Services for Purley Refresh Server Platforms 4.1.4.505.
8. Corrected typo in "PCIe PLL SSC" setup item help string.
9. Updated ePPR module from v3.01 to v3.03.
10. Removed 4G limit of Intel LAN memory if boot mode is not legacy.
11. Updated AEP firmware to FW_1.2.0.5446 and UEFI driver to 3515 for IPU2021.1.
12. Synced IPv6 status detection rule with BMC to make sure IPv6 status is the same in BIOS and BMC web.
13. Modified DCPMM gNfitBindingProtocolGuid installation timing to previous timing for compatibility with OOB timing.
14. Fixed problem of "Configuration Address Source" always showing "DHCP" on IPMI IPv6 page.
15. Corrected SMBIOS type 9 and fixed failure of type 40 to report M.2 on AOC-SLG3-2M2 for CPU1 slot1 (lane reversal).
16. Added RSC-P2-88 second slot SDL definition for IRQ assignment.
17. Corrected display of UEFI OS boot option name in BIOS setup.
18. Fixed problem of IPv6 disabling in the IPMI GUI but BIOS initialization showing IPv6 address.

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. Enabled support for SmcIntelAEP firmware update and updated AEP firmware to FW_1.2.0.5444 to match IPU2020.2.
14. 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).
15. Fixed problem of EFI version of PassMark MemTest86 hanging when SMCI Redfish Host Interface is not supported in IPMI firmware.
16. Fixed failure of "UEFI Compliant - Boot from iSCSI peripheral" in UEFI SCT test.
17. Fixed problem of system hanging during BIOS flash if Watch Dog function is enabled.
18. Fixed inability of 6240R and some refresh 4 serial CPU frequencies to reach maximum when enabling Mwait.
19. Corrected BMC firmware revision in BIOS Setup.
20. Fixed problem of system hanging at 0xB2 with some NVMe devices.
21. Fixed problem of system hanging at POST code 0xA0 or 0xA2 when using unsupported security NVMe device and installing Hyper-V with Windows 2019.
22. Fixed problem of system hanging at POST code"B2" when creating RAID0/1 volume.

3.3 (02/22/2020)

1. Updated BIOS ACM 1.7.40 and SINIT ACM 1.7.48 PW.
2. Added sighting CLX28 workaround and downgraded patrol scrub UC to CE.
3. Added SMC HDD Security feature.
4. 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).
5. Enhanced PPR log function.
6. Updated AMI label 5.14_PurleyCrb_0ACLA050 beta for IPU2020.1 PV.
7. Updated SPS_E5_04.01.04.381 from IPU 2020.1 PV.
8. Updated setup menu to remove our own tRFC optimization item, add Intel "tRFC Optimization for 16Gb Based DIMM" and "Panic and High Watermark" items, and add "Balanced Profile" option for "DCPMM Performance Setting".
9. Fixed Intel Self test 7 v111 SPI/DCh BIOS_CNTL to set BIOS Control Register BIT[9] to 1.
10. Fixed inability to log UPI correctable error.
11. Removed IMC Interleave from extreme performance mode if IMC Interleave is not AUTO.
12. Fixed malfunction of auto detection for AOC-SLG3-2M2 CPU1 slot1.
13. Fixed inability to create HTTP/HTTPS boot option when USB UNDI module is enabled.
14. Fixed failure of JBOF device detection.

3.2 (10/19/2019)

1. Updated AMI label 5.14_PurleyCrb_0ACLA049_BETA for BKC WW36 RC595.D04 Hot_FIX 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. 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. Enhanced support for Intel Speed Select.
13. Implemented dynamic change for Secure Boot Mode default value.
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. Removed PXE option for "OnBoard LanX Option ROM" when "Boot mode select" is UEFI.
22. Fixed inability of InBand Update BIOS in Linux OS to preserve Linux secureboot keys.
23. Corrected display of the IPMI AUX revision.
24. Fixed inability to identify duplicate boot options with more than one of the same M.2 AHCI interface devices.
25. Fixed problem of boot time increasing by more than two minutes per boot after running stress over hundreds of cycles.
26. Fixed inability to identify duplicate NVMe boot options with more than one of the same NVMe drives on an add-on card.
27. Changed OOB download and Upload Bios Configuration sequence.
28. Fixed problem of SMBIOS UUID MAC address partially showing 0xFF with Omni-path SIOM card.
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.
32. Removed SNC override when set to extreme performance mode.

33. Removed Intel Virtualization Technology override when set to extreme performance (in extreme performance mode support only).

3.1 (04/30/2019)

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. Fixed problem of system halting or rebooting at POST code 0xB2 or 0x92 when total GPT partition number is more than 256 and RSD is enabled.
9. Fixed inability to change IPv6 address or IPv6 Router1 IP address.

3.0c (3/30/2019)

1. Updated Intel BKCWW12 2019 PV MR4.
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. Added driver health warning message.
6. Hid Driver Health page for SUM.
7. Reduced redundant reboot for offboard VGA switching.
8. Set NVDIMM ADR timeout to 600µs.
9. Enhanced the solution for the error/warning message from dmidecode after a modification by AMIDE.
10. Improved behavior of "Monitor/MWAIT" & "Extreme/Maximum Performance".
11. Updated to SPS 4.1.02.174 or above for INTEL-SA-00185 Security Advisory and to RC 549.D13 or above for INTEL-SA-00192 Security Advisory.
12. Enhanced BIOS setup menu to auto-switch the Option ROM's value and hide the unexpected value when boot mode changes.
13. 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.
14. Set SDDC+1/ADDDC to enabled by default.
15. 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".
16. Corrected TPM RSD ChangeTPMState behavior to control TPM 1.2/2.0 state instead of "Security Device Support".
17. Fixed problem of TPM 2.0 device disappearing when disabling "RSD PSME ChangeTPMState API" and then enabling TPM 2.0 state.
18. Modified UEFI network description to IPv4/IPv6 to follow Industry Standard.
19. 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).
20. Fixed failure of NVMe hotplug function with BPN-ADP-12NVMe-2UB under Linux OS.
21. Fixed failure to log memory UCE event due to incorrect flag.
22. Fixed inability of "Network Stack"-related items to get/change via SUM OOB method.
23. Fixed incorrect display of the TDP of Intel Speed Select table.
24. Patched problem of incorrect memory power being reported in PTU.

25. Applied workaround for inability of SUM to get full setting of IODC setup item.
26. Temporarily fixed error for SKX (CLX) 4114 CPU memory training with Micron (18ASF2G72PDZ-2G6E1) RDIMM.

3.0a (2/20/2019)

1. Added support for Purley Refresh platform.
2. Updated SATA RAID OPROM/EFI driver to RSTe PreOS v6.0.0.1024.
3. Updated Giga LAN legacy PXE/legacy iSCSI OPROM driver to IBA 23.2 and uEFI driver to IBA 23.5.
4. Set BMC MAC address to UUID for system without onboard LAN1 or with onboard LAN1 disabled.
5. Set PCIe correctable and uncorrectable (non-fatal) error report to disabled by default.
6. Set RFC4122 encoding to only be enabled for build time produced by IPMI 1.29 or newer.
7. Updated CPU microcode SRV_P_264 for Skylake-SP H0/M0/U0 CPUs.
8. Updated valid range of IPMI setup item VLAN ID to 1-4094.
9. Added support for "Extreme Performance Mode" with 2U2Node backplane adapters.
10. Fixed problem of setup item "Quiet Boot" staying enabled after flashing BIOS with "Quiet Boot" disabled.

2.1a (9/15/2018)

1. Set PCIe link status to be polled at DXE stage to fix wrong information in BIOS setup IIO page.
2. Disabled "tRWSR Relaxation" by default.
3. Added support for Monitor Mwait feature.
4. Updated SPS 4.0.4.381 for INTEL-SA-00131 Security Advisory to address CVE-2018-3643 and CVE-2018-3644 security issues.
5. Fixed inability of VMD status to load default if loading default by AFU.
6. Updated CPU microcode SRV_P_253 for Skylake-SP H0/M0/U0 stepping CPUs.
7. Fixed missing sensor reading for add-on devices.
8. Fixed problem of BIOS always retrying boot when Re-Try Boot is Disabled.
9. Fixed malfunction of BIOS/ME downgrade check when running flash package (SWJPME2) a second time.
10. Fixed problem of system resetting while flashing BIOS under OS if Watch Dog function is enabled.
11. Fixed missing information for Hybrid backplane SMBIOS type 39.
12. Fixed failure of turbo in new Linux kernel.

2.1 (7/13/2018)

1. Updated CPU microcode to address 'Spectre' derivatives (CVE-2018-3639 & CVE-2018-3640) security issue.
2. Updated 5.12_PurleyCrb_0ACFD088 for Purley Skylake platform PLR7, BKC 2018 WW20.
3. Updated Giga LAN EFI driver 8.3.0.4 (IBA 23.1).
4. Updated SPS 4.00.04.340 PV PLR7 version.
5. Updated SATA RAID OPROM/EFI driver to RSTe PreOS v5.4.0.1039.
6. Corrected default setting for Enable SmcBusMasterEn setup item.
7. Corrected BIOS/ME downgrade check for SPS 4.0.4.340.
8. Added support for UEFI mode PXE boot of F12 hot key Net boot.
9. Added one event log to record that the event log is full.
10. Updated BIOS ACM 1.3.7 and SINIT ACM 1.3.4.
11. Fixed problem of SUM GetSataInfo showing incorrect "Configuration Type" when setting "Configure sSATA as" to "AHCI" or "RAID" on sSATA controller.

12. Fixed problem of Ctrl + Alt + Del causing system to hang after flashing BIOS.
13. Fixed missing NVDIMM ADR setup item.
14. Fixed problem of system hanging when installing Linux OS after COM1 & COM2 IO/IRQ exchange.

2.0b (2/24/2018)

1. Updated CPU microcode to address CVE-2017-5715 security patch issue.
2. Updated 5.12_PurleyCrb_0ACFD085Beta for Purley Skylake platform PLR 4, BKC WW02.
3. Added setup item "SmcBusMasterEn" for enabling Parent bridge of the devices in the gSmcPciForceEnableBusMasterList.
4. Changed RC default setting to upgrade POST Memory correctable error to uncorrectable error and map out the channel.
5. Added support for System Firmware Progress System Firmware Progress feature.
6. Fixed inability to reset the system under DOS by pressing "Ctrl-Alt-Del" on USB keyboard when "Port 60/64 Emulation" is disabled.
7. Fixed problem of SMC skipping first boot option in UEFI mode when retrying boot.
8. Fixed malfunction of "SMBIOS Preservation" Disabled.
9. Fixed issue of all commands requesting to be persistent.
10. Disabled CPU2 IIO PCIe root port ACPI hot plug function.
11. Fixed issue with IPMI force boot.
12. Fixed malfunction of option ROM control for AOC-MTG-i2TM and BPN-ADP-12NVMe-2UB.
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 incorrect LED behavior if VMD is disabled by stack but not by ports.