BIOS Release Notes Form

Product Name	**X11DPFF-SN**
Release Version	**3.8b SPS: 4.1.04.901**
Build Date	**01/06/2023**
Previous Version	**3.5**
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)

3.5 (5/21/2021)

1. *Added support for IPMI UEFI PXE boot to all LAN ports feature.*
2. *Enabled system to boot into PXE with DVD installed.*
3. *Updated SATA/sSATA EFI driver to VROC PreOS v7.5.0.1150.*
4. *Updated Intel Server Platform Services for Purley Refresh Server Platforms HF 4 PLR 4.1.4.450.*
5. *Added support for IPv6 HTTP Boot function.*
6. *Updated Skylake-SP/Cascade Lake-SP CPU PV microcode from Intel-Generic-Microcode-20210125_NDA.*
7. *Updated SATA/sSATA EFI driver to VROC PreOS v7.5.0.1152.*
8. *Removed 4G limit of Intel LAN memory if boot mode is not legacy.*
9. *Updated Skylake-SP/Cascade Lake-SP CPU beta microcode from IPU2021.1.*
10. *Added workaround for PCH SMBUS conflict when system has 3108 AOC and M.2 device on AOC-SLG3-2M2 is set to VMD mode.*
11. *Updated Skylake-SP/Cascade Lake-SP CPU PC microcode from IPU2021.1.*
12. *Synced IPv6 status detection rule with BMC to make sure IPv6 status is the same in BIOS and BMC web.*
13. *Enabled flash of FIT region by BtG projects while recovering.*
14. *Fixed problems with SERR/PERR from ASC-29320LPE on PCH slot.*
15. *Fixed problem of "Configuration Address Source" always showing "DHCP" on IPMI IPv6 page.*
16. *Modified DCPMM gNfitBindingProtocolGuid installation timing to previous timing for compatibility with OOB timing.*
17. *Fixed inability of BIOS to detect riser card when installing AOC-S100G-b2C after rebooting system.*
18. *Corrected display of UEFI OS boot option name in BIOS setup.*
19. *Fixed problem of IPv6 disabling in the IPMI GUI but BIOS initialization showing IPv6 address.*
20. *Fixed issue of BIOS getting wrong SMBIOS type 40 for some SIOM devices.*
21. *Fixed inability to report onboard LAN MAC address to IPMI when onboard LAN uses 64bit memory resource.*
22. *Corrected display of add-on card MAC.*

3.4 (11/4/2020)

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. Fixed problem of system hanging during BIOS flash if Watch Dog function is enabled.
14. Fixed inability of 6240R and some refresh 4 serial CPU frequencies to reach maximum when enabling Mwait.
15. Corrected BMC firmware revision in BIOS Setup.
16. Fixed problem of system hanging at 0xB2 with some NVMe devices.
17. 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 (10/8/2019)

1. Updated AMI label 5.14_PurleyCrb_0ACLA049_BETA for BKC WW36 IPU 2019.2 and AMI security update SA50072.
2. Updated SINIT/BIOS ACM from BKC WW36 IPU 2019.2 to address CVE-2019-0151 and CVE-2019-0152.

3. Updated SPS_E5_04.01.04.339.0 from BKC WW36 IPU 2019.2 to address PSIRT-TA-201905-011.
4. Updated Cascade Lake-SP CPU microcode and Skylake-SP microcode.
5. Changed "Secure Boot Mode" to ReadOnly attribute.
6. Displayed Setup item "ARI Support".
7. Set software threshold for non-fatal MCE error with yellow status to enabled as default.
8. Displayed CPU Flex Ratio-related setup items when the CPU on system supports IntelR Speed Select technology "Performance Profile" feature.
9. Added setup item to control 16Gb based Single Die Package DIMM tRFC optimization.
10. Patched inability of system to boot via onboard LAN2 after IPMI forces PXE boot when there is an OS behind LSI-3108 RAID card.
11. Updated the behavior for the feature that updates SMBIOS Type 1 and 3 with FRU0.
12. Added Enhanced PPR function and set disabled as default.
13. Corrected display of the IPMI AUX revision.
14. Corrected sequence of Boot Order.
15. Fixed problem of two OS (Redhat & Ubuntu) boot devices appearing in boot order.
16. Set ADDDC to enabled by default.

3.1a (09/06/2019)

1. Updated Skylake-SP/Cascade Lake-SP CPU microcode.
2. Updated new KTI value for SKX and CLX CPU.
3. Updated AMI label 5.14_PurleyCrb_0ACLA048_BETA for WW26 BKC PLR2.
4. Updated SPS_E5_04.01.04.323.0 from BKC WW26 2019.
5. Changed UEFI LAN Boot option name format.
6. Moved code for masking Mwait instruction to end of POST.
7. Added recommended AEP DIMM firmware version.
8. Updated VBIOS and VGA EFI Driver to 1.10.
9. Displayed Setup item "ARI Support".

3.1 (5/8/2019)

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. Set PCIe correctable and uncorrectable (non-fatal) error report to disabled by default.
9. Added support for Linux built-in utility efibootmgr.
10. Updated valid range of IPMI setup item VLAN ID to 1-4094.
11. Added driver health warning message.
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. Changed OPROM settings to EFI for OEM BIOS that only changes the boot mode to UEFI without other changes.
15. Enhanced F12 hot key PXE boot feature.
16. Set ADDDC Sparing to enabled by default.

17. Fixed inability to change IPv6 address or IPv6 Router1 IP address.
18. Fixed failure of CPU PBF (Prioritized Base Frequency).
19. Added workaround for failure of BIOS flash with 156 bytes PubKey (Error: "Secure Flash Rom Verify Fail").
20. Modified UEFI network description to IPv4/IPv6 to follow Industry Standard.
21. Applied workaround for inability of SUM to get full setting of IODC setup item.
22. Fixed failure to boot into VMware OS when set to Maximum Performance even if Monitor/MWAIT is enabled.
23. Fixed the missing asset information with AOC-MTG-i2T SIOM.

3.0a (3/22/2019)

1. Added support for Purley Refresh platform.
2. Updated SATA RAID OPROM/EFI driver to RSTe PreOS v6.0.0.1024.
3. Added support for Monitor Mwait feature.
4. Patched missing PSU information if backplane MCU reports wrong PSU information.
5. Set BMC MAC address to UUID for system without onboard LAN1 or with onboard LAN1 disabled.
6. Hid setup item "L2 RFO Prefetch Disable" to adhere to draft template v0.7.
7. Changed BIOS revision to 3.0a.
8. Enabled RFC4122 UUID support.
9. Fixed malfunction of disabling Watch Dog while flashing BIOS under OS.
10. Fixed problem of BIOS always retrying boot when Re-Try Boot is Disabled.
11. Fixed malfunction of support for LEGACY to EFI.
12. Fixed failure of always turbo in new Linux kernel 7.2.
13. Fixed problem of system hanging and falling into a dead loop when setting enabled CPU core number to 1 in always turbo mode.
14. Fixed problem of CPU core numbers and maximum turbo ratio not matching in always turbo mode.
15. Fixed inability of user to configure VMD setting for M.2 ports.

_____ _____

Product Manager *Date*