BIOS Release Notes Form

Product Name	**X11DPFR-S(N)**
Release Version	**3.8a SPS: 4.1.04.804**
Build Date	**10/28/2022**
Previous Version	**3.6**
Update Category	**Recommended**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Updated AMI label 5.14_PurleyCrb_0ACLA057 for RC0623.D09 2022.3 IPU.** **2. Updated token RC_VERSION_VALUE setting to 623.D09.** **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.** **5. In the event log page, the fix displays the wrong DIMM location.** **6. Modified String naming from SMCI to Supermicro.** **7. "Vendor Keys" have been removed from the security page.** **8. a.) Refined SMM buffer validation in SmmSmbiosELogInitFuncs.c.** **b.) In DxeSmmRedirFuncs.c, a runtime buffer was allocated to trigger ELog SMI.** **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 legacy driver to VROC PreOS v6.3.5.1003 Hot Fix to fix 10TB or higher volume drive issue.** **11. 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), CVE-2022-25976 (5.5 Medium).** **12. Modified the allocated buffer from EfiBootServicesData to EfiRuntimeServicesData.**
New features	**N/A**
Fixes	**1. Enabled IScsi_SUPPORT on Purley generation.**

Release Notes from Previous Release(s)

3.6 (1/21/2022)

1. *Change 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 the 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.*

3.5 (6/1/2021)

1. Updated 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 and 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. Added support for IPMI UEFI PXE boot to all LAN ports feature.
6. Updated SATA/sSATA EFI driver to VROC PreOS v7.5.0.1152.
7. Enabled system to boot into PXE with DVD installed.
8. Updated Intel Server Platform Services for Purley Refresh Server Platforms HF 4 PLR 4.1.4.450.
9. Added support for IPv6 HTTP Boot function.
10. Corrected typo in "PCIe PLL SSC" setup item help string.
11. Removed 4G limit of Intel LAN memory if boot mode is not legacy.
12. Updated AEP firmware to FW_1.2.0.5446 and UEFI driver to 3515 for IPU2021.1.
13. Synced IPv6 status detection rule with BMC to make sure IPv6 status is the same in BIOS and BMC web.
14. Fixed problem of "Configuration Address Source" always showing "DHCP" on IPMI IPv6 page.
15. Corrected display of UEFI OS boot option name in BIOS setup.

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 problem of system hanging during BIOS flash if Watch Dog function is enabled.
16. Fixed inability of 6240R and some refresh 4 serial CPU frequencies to reach maximum when enabling Mwait.
17. Corrected BMC firmware revision in BIOS Setup.
18. Fixed problem of system hanging at 0xB2 with some NVMe devices.
19. 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 (02/21/2020)

1. Updated BIOS ACM 1.7.40 and SINIT ACM 1.7.48 PW.
2. 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).
3. Updated AMI label 5.14_PurleyCrb_0ACLA050 beta for IPU2020.1 PV.
4. Updated SPS_E5_04.01.04.381 from IPU 2020.1 PV.
5. Added setup item "HDD password prompt Control" to control "Hard-Drive Password Check" for enabling/disabling HDD password prompt window during POST.
6. Enhanced PPR log function.
7. Fixed inability to log UPI correctable error.
8. Removed IMC Interleave from extreme performance mode if IMC Interleave is not AUTO.
9. Fixed inability to create HTTP/HTTPS boot option when USB UNDI module is enabled.

3.2 (10/16/2019)

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. 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. Removed PXE option for "OnBoard LanX Option ROM" when "Boot mode select" is UEFI.
23. Fixed inability of InBand Update BIOS in Linux OS to preserve Linux secureboot keys.
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. 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 (3/28/2019)

1. Updated Intel BKCWW10 2019 PV MR3.
2. Updated SPS_E5_04.01.04.256.0 from BKC WW08 2019.
3. Updated Skylake-SP/Cascade Lake-SP CPU microcode from SRV_P_272.
4. Updated standard NVDIMM ADR time.
5. Set PCIe correctable and uncorrectable (non-fatal) error report to disabled by default.
6. Disabled unused SPS ME "CUPS IIO" and "Volumetric Airflow" sensor.
7. Added support for Linux built-in utility efibootmgr.
8. Updated valid range of IPMI setup item VLAN ID to 1-4094.

9. Added driver health warning message.
10. 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.
11. Enhanced BIOS setup menu to auto-switch the Option ROM's value and hide the unexpected value when boot mode changes.
12. 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.
13. Fixed failure of CPU PBF (Prioritized Base Frequency).
14. Added workaround for failure of BIOS flash with 156 bytes PubKey (Error: "Secure Flash Rom Verify Fail").
15. Modified UEFI network description to IPv4/IPv6 to follow Industry Standard.
16. Applied workaround for inability of SUM to get full setting of IODC setup item.
17. Fixed failure to boot into VMware OS when set to Maximum Performance even if Monitor/MWAIT is enabled.
18. Temporarily fixed error for SKX (CLX) 4114 CPU memory training with Micron (18ASF2G72PDZ-2G6E1) RDIMM.

3.0a (1/12/2019)

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_262 for Skylake-SP H0/M0/U0 CPUs.
8. Disabled unused SPS ME "CUPS IIO" and "Volumetric Airflow" sensor.
9. Added support for Linux built-in utility efibootmgr.
10. Updated valid range of IPMI setup item VLAN ID to 1-4094.
11. Fixed problem of setup item "Quiet Boot" staying enabled after flashing BIOS with "Quiet Boot" disabled.

2.1a (10/23/2018)

1. Added support for Monitor Mwait feature.
2. Fixed inability of VMD status to load default if loading default by AFU.
3. Updated SATA RAID OPROM/EFI driver to RSTe PreOS v5.5.0.1028.
4. Updated SPS 4.0.4.393 to correct problems of unexpected SPS response to HECI Host Config cmd with PStatesRatio Missing when HWPM is enabled as OOB or Native without legacy, and of duplicated EID being assigned on MCTP endpoint after sending MCTP force discovery IPMI command.
5. Updated SATA RX DWORD20 Ports 0, 1, 2, 4, 5, and 6 to ~2.4dB and ports 3 and 7 to ~1.6dB.
6. Synchronized setup menu string and SMBIOS type9 slot description.
7. Fixed problem of system resetting while flashing BIOS under OS if Watch Dog function is enabled.
8. Fixed malfunction of BIOS/ME downgrade check when running flash package (SWJPME2) a second time.
9. Fixed problem of BIOS always retrying boot when Re-Try Boot is Disabled.
10. Fixed malfunction of support for LEGACY to EFI.
11. Fixed issue with IPMI firmware capability.
12. Fixed failure of turbo in new Linux kernel.
13. Fixed inability to set memory policy.

14. Fixed problem of setup item "Quiet Boot" staying enabled after flashing BIOS with "Quiet Boot" disabled.
15. Fixed problem of system hanging after downgrading BIOS from 2.1a to 2.1.

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_0ACFD088Beta for Purley Skylake platform PLR7, BKC 2018 WW20.
3. Corrected default setting for Enable SmcBusMasterEn setup item.
4. Added hidden item "Early Console Logo".
5. Added support for RFC3021.
6. Updated BIOS ACM 1.3.7 and SINIT ACM 1.3.4.
7. Fixed problem of Ctrl + Alt + Del causing system to hang after flashing BIOS.
8. Fixed problem of SUM GetSataInfo showing incorrect "Configuration Type" when setting "Configure sSATA as" to "AHCI" or "RAID" on sSATA controller.
9. Fixed problem of the NVMe drivers not showing temperature and ejecting when only one CPU is installed and AOC-SLG3-2E4T is on CPU1 RP1.
10. Fixed problem of DMI being cleared when running SUM UpdateBios.
11. Displayed setup items for JEDEC NVDIMM.

2.0b (2/24/2018)

1. Implemented enhancement to address 'Spectre' variant 2 (CVE 2017-5715) security patch issue.
2. Changed maximum speed in SMBIOS type 4 to 4500Mhz.
3. Added support for AOC-SLG3-2E4T only for two NVMe drives.
4. Added support for System Firmware Progress System Firmware Progress feature.
5. Added support for BPN-SAS3-F424-A6N4 panel for six NVMe drives.
6. Fixed inability of some CPUs to display correct microcode revision under BIOS setup menu.