IPMI Firmware / BIOS Release Notes Form

Product Name	**X11DPU-V**
Release Version	**4.0**
Release Date	**6/20/2023**
Previous Version	**3.7**
Update Category	**Critical**
Dependencies	**None**
Important Notes	**None**
Enhancement	**1.[Enhancements] Update AMI label 5.14_PurleyCrb_0ACLA056 for RC0622.D07 2022.2 IPU.** **2.[Enhancements] Updated Skylake-SP/Cascade Lake-SP CPU PC microcode for IPU 2022.1.** **3.[Enhancements] Update token RC_VERSION_VALUE setting to 622.D07. Update token PRICESSO_0_UCODE_VERSION setting to 02006E05. Update token FW_SPS_VERSION setting to 4.1.4.804.** **4.[Enhancements] Fix show wrong DIMM location in event log page.** **5.[Enhancements] Modify String naming from SMCI to Supermicro.** **6.[Enhancements] Remove "Vendor Keys" in security page.** **7.[Enhancements] Modify the allocated buffer from EfiBootServicesData to EfiRuntimeServicesData.** **8.[Enhancements] Disable MROM1 device since product doesn't use Intel IE function.**

	9.[Enhancements] Update DBX file to fix Secure Boot Bypass issue. **10.[Enhancements] Update VROC SATA/sSATA EFI driver to VROC PreOS v7.8.0.1012 to address 1. Data Loss Exposure Due to RAID 5 TRIM Support. Document #737276. 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)** **11.[Enhancements] Change BIOS revision to 4.0.** **12.[Enhancements] Update AMI label 5.14_PurleyCrb_0ACLA060 for RC0628.P50 IPU 2023.3 (1). For INTEL-SA-00813 Security Advisory to address CVE-2022-37343(7.2, High), CVE-2022-44611(6.9, Medium), CVE-2022-38083(6.1, Medium), CVE-2022-27879(5.3, Medium) and CVE-2022-43505(4.1, Medium) security issues. (2). For INTEL-SA-00828 Security Advisory to address CVE-2022-40982(6.5, Medium) security issue.** **13.[Enhancements] Update token RC_VERSION_VALUE setting to 628.P50. Update token PRICESSO_0_UCODE_VERSION setting to 02007006. Update token PRICESSO_2_UCODE_VERSION setting to 04003604. Update token PRICESSO_3_UCODE_VERSION setting to 05003604. Update token FW_SPS_VERSION setting to 4.1.5.2.** **14.[Enhancements] Updated Cascade Lake-SP CPU PV microcode for IPU 2023.3.** **15.[Enhancements] Updated Intel Server Platform Services for Purley Refresh Server Platforms IPU2023.3 4.1.5.2**
New features	**N/A**
Fixes	**N/A**

Release Notes from Previous Release(s)

3.7(6/15/2022) *1.[Enhancements] Change BIOS revision to 3.6.* *2.[Enhancements] Update SATA/sSATA EFI driver to VROC PreOS v7.7.0.1054.* *3.[Enhancements] Update AEP uEFI driver to 1.0.0.3531 for IPU2021.2.*

4.[Enhancements] Update AMI label 5.14_PurleyCrb_0ACLA054 for RC0616.D08 2021.2 IPU. For INTEL-SA-00527 Security
Advisory to address CVE-2021-0103(8.2, High), CVE-2021-0114(7.9, High), CVE-2021-0115(7.9, High), CVE-2021-0116(7.9,
High), CVE-2021-0117(7.9, High), CVE-2021-0118(7.9, High), CVE-2021-0099(7.8, High), CVE-2021-0156(7.5, High), CVE-
2021-0111(7.2, High), CVE-2021-0107(7.2, High), CVE-2021-0125(6.7, Medium), CVE-2021-0124(6.3, Medium), CVE-2021-
0119(5.8, Medium), CVE-2021-0092(4.7, Medium), CVE-2021-0091(3.2, Low) and CVE-2021-0093(2.4, Low) security issues.
5.[Enhancements] Updated Intel Server Platform Services for Purley Refresh Server Platforms IPU2021.2 HF1 4.1.4.654.
6.[Enhancements] Update BIOS ACM 1.7.51, SINIT ACM 1.7.51 PW. For INTEL-SA-00527 Security Advisory to address CVE-
2021-0103(8.2, High), CVE-2021-0114(7.9, High), CVE-2021-0115(7.9, High), CVE-2021-0116(7.9, High), CVE-2021-0117(7.9,
High), CVE-2021-0118(7.9, High), CVE-2021-0099(7.8, High), CVE-2021-0156(7.5, High), CVE-2021-0111(7.2, High), CVE-
2021-0107(7.2, High), CVE-2021-0125(6.7, Medium), CVE-2021-0124(6.3, Medium), CVE-2021-0119(5.8, Medium), CVE-2021-
0092(4.7, Medium), CVE-2021-0091(3.2, Low) and CVE-2021-0093(2.4, Low) security issues.
7.[Enhancements] Updated Skylake-SP/Cascade Lake-SP CPU PV microcode. Updated Skylake-SP H0/M0/U0 stepping CPU
PV microcode MB750654_02006C0A. Update Cascade Lake-SP B0 stepping CPU PV microcode MBF50656_0400320A.
Update Cascade Lake-SP B1 stepping CPU PV microcode MBF50657_0500320A. For INTEL-SA-00532 Security Advisory to
address CVE-2021-0127(5.6, Medium) security issue. For INTEL-SA-00365 Security Advisory to address CVE-2020-8673(4.7,
Medium) security issue.
8.[Enhancements] Change BIOS revision to 3.7.
9.[Enhancements] Update VROC SATA/sSATA legacy driver to VROC PreOS v6.3.5.1003 Hot Fix to fix 10TB or higher volume
drive issue.
10.[Enhancements] Update AEP uEFI driver to 01.00.00.3534 for IPU2022.2.
11.[Enhancements] Update AMI label 5.14_PurleyCrb_0ACLA055 for RC0618.D03 2022.1 IPU. (1). 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. (2). 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. (3). For INTEL-SA-00616 Security Advisory
to address CVE-2021-21131(3.3, Low) and CVE-2021-21136(2.7, Low) security issues.

12.[Enhancements] Updated Skylake-SP/Cascade Lake-SP CPU PC microcode for IPU 2022.1. (1). 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. (2). 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. (3). For INTEL-SA-
00616 Security Advisory to address CVE-2021-21131(3.3, Low) and CVE-2021-21136(2.7, Low) security issues.
13.[Enhancements] Update BIOS ACM 1.7.54, SINIT ACM 1.7.55 PW for IPU2022.1 to address
14.[Enhancements] Updated Intel Server Platform Services for Purley Refresh Server Platforms IPU2022.1 4.1.4.700
15.[Enhancements] Following PM request, rollback AOC-SLG3-4E4R re-driver settings to 3.5.

3.4(11/03/2020)
1.[Enhancements]Update 5.14_PurleyCrb_0ACLA052_BETA for RC update and 2020.2 IPU PV to addresses Intel-TA-00358: CVE-2020-0587 (6.7 Medium), CVE-2020-0591 (6.7 Medium), CVE-2020-0592 (3 Low), 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), CVE-2020-8764 (8.7 High) INTEL-TA-00391: CVE-2020-8752(9.4, Critical), CVE-2020-8753(8.2, Critical), CVE-2020-12297(8.2, Critical), CVE-2020-8745(7.3, Critical), CVE-2020-8705(7.1, Critical), CVE-2020-12303(7.0, Critical), CVE-2020-8757(6.3, Medium), CVE-2020-8756(6.3, Medium), CVE-2020-8760(6.0, Medium), CVE-2020-8754(5.3, Medium), CVE-2020-8747(4.8, Medium), CVE-2020-12356(4.4, Medium), CVE-2020-8746(4.3, Medium), CVE-2020-8749(4.2, Medium). INTEL-SA-00358: CVE-2020-0590(7.7, High), CVE-2020-0587(6.7, Medium), CVE-2020-0591(6.7, Medium), CVE-2020-0593(4.7, Medium), CVE-2020-0588(3.8, Low), CVE-2020-0592(3.0, Low). INTEL-TA-00391: CVE-2020-8744(7.2, High), CVE-2020-8705(7.1, High), CVE-2020-8755(4.6, Medium). AMI SA50080 and AMI SA50081: CVE-2020-0570(7.6, High), CVE-2020-0571(5.5, Medium) and CVE-2020-8675(7.1, High). AMI SA-50085: CVE-2020-10713 (8.2, High) AMI SA-50084: CVE-2020-10255 (9, High)
2.[Enhancements]Enable token "IPMI_FORCE_BOOT_UEFI_SHELL" to support to shell by ipmi change boot order command.
3.[Enhancements] Move all LANs to the top of boot priority when IPMI force PXE.
4.[Enhancements][SmcHttpBoot] Delete repeated boot options which have description the same as the new description.
5.[Enhancements] Add inband flash status event log to IPMI MEL.
6.[Enhancements] Correct "Station MAC Address" display order when "Configuration Address Source" set to "Static".
7.[Enhancements] Update SATA/sSATA RAID OPROM/EFI driver to VROC PreOS v6.3.0.1005 PV.
8.[Fixes] Fix 6240R and some refresh 4 serial CPU freq. can't reach the highest when enabling mwait.
9. .[Fixes] Fixed Secure Erase - Password doesn't success and BIOS return "EFI_Device_Error" with SED: Seagate ST1000NX0353.
10.[Fixes]firmware revision may not correct in BIOS Setup.
11.[Fixes] Fixed System hang 0xB2 problem with some NVME device.
12.[SmcRedfishHostInterface][Fixes] Fixed EFI version of PassMark MemTest86 hangs up when SMCI Redfish Host Interface is not supported in IPMI FW.

3.3 (03/06/2020)

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. Displayed Setup item "ARI Support".
6. Added setup item to control 16Gb based Single Die Package DIMM tRFC optimization.
7. Updated Secure Boot Key to fix the error message of PK key.
8. Patched inability of system to boot via onboard LAN2 after IPMI forces PXE boot when there is an OS behind LSI-3108 RAID card.
9. Added back erase NVDIMM routine.
10. Updated VBIOS and VGA EFI Driver to 1.10.
11. Enhanced F12 hot key PXE boot feature.
12. Updated the behavior for the feature that updates SMBIOS Type 1 and 3 with FRU0.
13. Disabled ADDDC/SDDC and set PPR as hPPR.
14. Enabled saving memory CE location into PPR variable at runtime even if memory correctable error reporting is disabled.
15. Added sighting CLX28 workaround and downgraded patrol scrub UC to CE.
16. Added SMC HDD Security feature.
17. Updated AMI label 5.14_PurleyCrb_0ACLA050 beta for IPU2020.1 PV.
18. Updated SPS_E5_04.01.04.381 from IPU 2020.1 PV.
19. Updated BIOS ACM 1.7.40 and SINIT ACM 1.7.48 PW.
20. Added setup item "HDD password prompt Control" to control "Hard-Drive Password Check" for enabling/disabling HDD password prompt window during POST.
21. 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).
22. Added Enhanced PPR function and set disabled as default.
23. Removed PXE option for "OnBoard LanX Option ROM" when "Boot mode select" is UEFI.
24. Corrected display of the IPMI AUX revision.
25. Changed OOB download and Upload Bios Configuration sequence.
26. Fixed problem of two OS (Redhat & Ubuntu) boot devices appearing in boot order.
27. Fixed failure of OPROM control item if CSM is disabled.
28. Removed Intel Virtualization Technology override when set to extreme performance (in extreme performance mode support only).
29. Fixed mismatch of Secure Boot Mode value.
30. Removed requirement to use Admin password for erasing TCG device.
31. Fixed problem of two CentOS boot items occurring in boot order if CentOS is installed in RAID 1 system.

3.1 (05/13/2019)

1. Added support for Purley Refresh platform.
2. Enhanced BIOS setup menu to auto-switch the Option ROM's value and hide the unexpected value when boot mode changes.
3. Updated to SPS 4.0.04.381 or above for INTEL-SA-00213 Security Advisory.
4. Updated Skylake-SP/Cascade Lake-SP CPU microcode.
5. Updated Intel BKCWW16 2019 PV PLR1.

6. Updated SPS_E5_04.01.04.296.0 from BKC WW16 2019.
7. Updated EIP467272 for AMI SA50069, SA50070.
8. Set SDDC Plus One or SDDC to disabled by default.
9. Updated SATA/sSATA RAID OPROM/EFI driver to VROC PreOS v6.1.0.1017.
10. Set Leaky Bucket that can decrease one memory correctable error count within 2.15 minutes with threshold 512.
11. Fixed problem of UUID showing IPMI MAC incorrectly after disabling onboard LAN chip.
12. Temporarily fixed error for SKX (CLX) 4114 CPU memory training with Micron (18ASF2G72PDZ-2G6E1) RDIMM.
13. Fixed failure to boot into VMware OS when set to Maximum Performance even if Monitor/MWAIT is enabled.
14. 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.
15. Fixed inability to change IPv6 address or IPv6 Router1 IP address.

3.0b(03/04/2018)
1. Supported Purley Refresh platform.
2. Update SATA RAID OPROM/EFI driver to RSTe PreOS v6.0.0.1024.
3. Set BMC MAC Address to UUID for system without onboard LAN1 or with onboard LAN1 disabled.
4. To disable pcie correctable and uncorrectable(non fatal) error report by default.
Will enable it with AERON(PCI AER Support).
5. Support RFC4122 UUID format feature, RFC4122 encoding from build time produced by IPMICFG 1.29 tool or newer version.
6. Update CPU microcode SRV_P_262 for Skylake-SP H0/M0/U0 CPUs.
7. Disable unused SPS ME "CUPS IIO" and "Volumetric Airflow" sensor.
8. Add 2933 to memory POR.
9. Support Linux built-in utility efibootmgr.
10. Update IPMI setup item VLAN ID valid range to 1~4094. (refer IEEE 802.1q standard).
11. Add driver health warning message.
12. Set NVDIMM ADR timeout to 600us.
13. Updated to SPS 4.1.02.174 or above for INTEL-SA-00185 Security Advisory. Updated to RC 549.D13 or above for INTEL-SA-00192 Security Advisory.
14. Fixed setup item "Quiet Boot" will keep enabled after flash BIOS which has "Quiet Boot" disabled.
15. Fixed PBF high frequency core number incorrect when Hyper-Threading disabled.
16. Workaround for BIOS flash fail with 156 bytes PubKey(Error: "Secure Flash Rom Verify Fail").
17. Modify UEFI network description as IPv4/IPv6 to follow Industry Standard.
18. Patched system hang 0x94 when plug NVIDIA Tesla T4 card.

1.0 (11/12/2018)
1. First Release.