IPMI Firmware / BIOS Release Notes Form

Supermicro disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade. All products, computer systems, dates, and figures specified are preliminary based on current expectations, and are subject to change without notice. Supermicro and the Supermicro logo are trademarks of Super Micro Computer, Inc. in the U.S. and/or other countries. Copyright © 2018 Super Micro Computer, Inc. All rights reserved.

Product Name	**X11DPT-L**
Release Version	**4.0**
Release Date	**11/29/2023**
Previous Version	**3.8a**
Update Category	**Recommended**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1.[Enhancements] Update AMI label 5.14_PurleyCrb_0ACLA058 for RC0626.P01 IPU 2023.1 (1). For INTEL-SA-00717 Security Advisory to address CVE-2022-32231 (7.5, High) / CVE-2022-26343 (8.2, High) security issues.** **2.[Enhancements] Update token RC_VERSION_VALUE setting to 626.P01.** **3.[Enhancements] Updated Cascade Lake-SP CPU PV microcode for IPU 2023.1.** **4.[Enhancements] Update AMI label 5.14_PurleyCrb_0ACLA059 for RC0627.P11 IPU 2023.2 (1). For INTEL-SA-00807 Security Advisory to address CVE-2022-38087(4.1, Medium) and CVE-2022-33894(7.5, High) security issues.** **5.[Enhancements] Update token RC_VERSION_VALUE setting to 627.P11. Update token PRICESSO_0_UCODE_VERSION setting to**

	02006F05. Update token PRICESSO_1_UCODE_VERSION setting to 03000012. Update token PRICESSO_2_UCODE_VERSION setting to 04003501. Update token PRICESSO_3_UCODE_VERSION setting to 05003501. 6.[Enhancements] Updated Cascade Lake-SP CPU PV microcode for IPU 2023.2. 7.[Enhancements] Change BIOS revision to 4.0. 8.[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. 9.[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. 10.[Enhancements] Updated Cascade Lake-SP CPU PV microcode for IPU 2023.3. 11.[Enhancements] Updated Intel Server Platform Services for Purley Refresh Server Platforms IPU2023.3 4.1.5.2 12.[Enhancements] Update DBX file for AMI-SA50182 SecureBoot DBX Update
New features	**N/A**
Fixes	N/A

Release Notes from Previous Release(s)

3.8a(2/7/2023)

1.[Enhancements] Update AMI label 5.14_PurleyCrb_0ACLA057 for RC0623.D09 2022.3 IPU. (1) 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), CVE-2022-29515(6.0 Medium) security issues. (2) For INTEL-TA-00688 Security Advisory to address CVE-2022-26006 (8.2 High), CVE-2022-21198(7.9 High) security issues.

2.[Enhancements] Update token RC_VERSION_VALUE setting to 623.D09. Update token PRICESSO_0_UCODE_VERSION setting to 02006E05. Update token FW_SPS_VERSION setting to 4.1.4.804.

3.[Enhancements] Update Intel DCPM UEFI driver to 1.0.0.3536.

4.[Fixes] Fix OA2 key injection issue.

5.[Enhancements] Updated Skylake-SP/Cascade Lake-SP CPU PC microcode for IPU 2022.2. (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.

6.[Enhancements] Fix show wrong DIMM location in event log page.

7.[Enhancements] Modify String naming from SMCI to Supermicro.

8.[Enhancements] Remove "Vendor Keys" in security page.

9.[Enhancements] [SMIHandlerSecurityFix] 1.Refine SMM buffer validation in SmmSmbiosELogInitFuncs.c 2.Allocate runtime buffer to trigger ELog SMI in DxeSmmRedirFuncs.

10.[Enhancements] Update 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)

11.[Enhancements] Update VROC SATA/sSATA legacy driver to VROC PreOS v6.3.5.1003 Hot Fix to fix 10TB or higher volume drive issue.

12.[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)

13.[Enhancements] Modify the allocated buffer from EfiBootServicesData to EfiRuntimeServicesData.

14.[Enhancements] Disable MROM1 device since product doesn't use Intel IE function.

15.[Enhancements] Update DBX file to fix Secure Boot Bypass issue.

16.[Enhancements] Support IPMI UEFI PXE boot to all LAN port feature.

17.[Fixes] Fix "Configuration Address Source" always show "DHCP" in IPMI IPv6 page.

18.[Enhancements] This system cannot boot into PXE with DVD installed.

19.[Enhancements] Support IPv6 HTTP Boot function.

20.[Enhancements] Correct typo in "PCIe PLL SSC" setup item help string.

21.[Fixes] Fixed UEFI OS boot option name shows incorrectly in BIOS setup.

22.[Enhancements] Remove intel lan memory 4G limit if boot mode is not legacy.

23.[Enhancements] Sync IPv6 status detection rule with BMC to make sure IPv6 status is the same in BIOS and BMC web.

3.4(8/26/2021)

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.[SmcRedfishHostInterface][Fixes] Fixed EFI version of PassMark MemTest86 hangs up when SMCI Redfish Host Interface is not supported in IPMI FW.
5.[Enhancements] Update SATA/sSATA RAID OPROM/EFI driver to VROC PreOS v6.3.0.1005 PV.
6.[Enhancements] Update AEP FW to FW_1.2.0.5444 to match IPU2020.2.
7.[Enhancements][SmcHttpBoot] Delete repeated boot options which have description the same as the new description.
8.[Fixes] Fixed Secure Erase - Password doesn't success and BIOS return "EFI_Device_Error" with SED: Seagate ST1000NX0353.
9.[Fixes]firmware revision may not correct in BIOS Setup.
10.[Fixes] Fixed System hang 0xB2 problem with some NVME device.
11.[Enhancements] Add inband flash status event log to IPMI MEL.
12.[Enhancements] Correct "Station MAC Address" display order when "Configuration Address Source" set to "Static".

3.3 (3/20/2020)
1 [Enhancements] Update AMI label 5.14_PurleyCrb_0ACLA050 beta for IPU2020.1 PV.
2 [Enhancements] Update BIOS ACM 1.7.40, SINIT ACM 1.7.48 PW
3 [Fixes] Fixed Secure Boot Mode value mismatch.
4 [Enhancements] To save memory ce location into PPR variable at runtime even if memory correctable error reporting is disabled.
5 [Fixes] Fix onboard SAS option ROM control not functioning
6 [Enhancements] Adding sighting CLX28 workaround, downgrade patrol scrub UC to CE.
7 [Enhancements] Updated Skylake-SP/Cascade Lake-SP CPU microcode from Intel-Restricted-2020-1-IPU limit beta.
8 [Fixes] Fix Intel Self test 7 v111 SPI/DCh BIOS_CNTL - BIOS Control Register BIT[9] should be set to 1.
9 [Enhancements] Add SMC HDD Security feature.
10 [Fixes] Could not log UPI correctable error.
11 [Fixes] Fixed system stops at post code 0x92 with Apacer M.2 SSD.
12 [Fixes] There is no need to use Adminword for erasing TCG device.
13 [Fixes] Fix two CentOS boot items in boot order if CentOS installed in RAID 1 system.
14 [Enhancements] Updated SPS_E5_04.01.04.381 from IPU 2020.1 PV
15 [Enhancements] Adding setup item "HDDword prompt Control" to control "Hard-Driveword Check" enable/disable HDDword prompt window during POST.
16 [Enhancements] Update Setup menu. 1) Remove our own tRFC optimization item, added Intel "tRFC Optimization for 16Gb Based DIMM", "Panic and High Watermark" item. 2) Added "Balanced Profile" option for "DCPMM Performance Setting"

3.2 (10/17/2019)

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. Set SDDC Plus One or SDDC to disabled by default.
6. Updated SATA/sSATA RAID OPROM/EFI driver to VROC PreOS v6.1.0.1017.
7. Set Leaky Bucket that can decrease one memory correctable error count within 2.15 minutes with threshold 512.
8. Enhanced F12 hot key PXE boot feature.
9. Updated AMI label 5.14_PurleyCrb_0ACLA049_BETA for BKC WW36 IPU 2019.2 and AMI security update SA50072.
10. Updated SINIT/BIOS ACM from BKC WW36 IPU 2019.2 to address CVE-2019-0151 and CVE-2019-0152.
11. Updated SPS_E5_04.01.04.339.0 from BKC WW36 IPU 2019.2 to address PSIRT-TA-201905-011.
12. Updated Cascade Lake-SP CPU microcode and Skylake-SP microcode.
13. Displayed Setup item "ARI Support".
14. Added setup item to control 16Gb based Single Die Package DIMM tRFC optimization.
15. Updated Secure Boot Key to fix the error message of PK key.
16. Patched inability of system to boot via onboard LAN2 after IPMI forces PXE boot when there is an OS behind LSI-3108 RAID card.
17. Added back erase NVDIMM routine.
18. Updated VBIOS and VGA EFI Driver to 1.10.
19. Enhanced F12 hot key PXE boot feature.
20. Updated the behavior for the feature that updates SMBIOS Type 1 and 3 with FRU0.
21. Added support for SMC HttpBoot.
22. Disabled ADDDC/SDDC and set PPR as hPPR.
23. Added Enhanced PPR function and set disabled as default.
24. 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.
25. Fixed inability to change IPv6 address or IPv6 Router1 IP address.
26. Set ADDDC to enabled by default.
27. Removed PXE option for "OnBoard LanX Option ROM" when "Boot mode select" is UEFI.
28. Corrected display of the IPMI AUX revision.
29. Changed OOB download and Upload Bios Configuration sequence.
30. Fixed problem of two OS (Redhat & Ubuntu) boot devices appearing in boot order.
31. Fixed failure of OPROM control item if CSM is disabled.

3.1 (5/21/2019)

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. Set SDDC Plus One or SDDC to disabled by default.
6. Updated SATA/sSATA RAID OPROM/EFI driver to VROC PreOS v6.1.0.1017.
7. Set Leaky Bucket that can decrease one memory correctable error count within 2.15 minutes with threshold 512.
8. Enhanced F12 hot key PXE boot feature.

9. Improved help messages of Intel VMD.
10. 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.
11. Fixed inability to change IPv6 address or IPv6 Router1 IP address.
12. Set ADDDC to enabled by default.

3.0c (3/27/2019)

1. Added support for Purley Refresh platform.
2. 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.
3. Enhanced BIOS setup menu to auto-switch the Option ROM's value and hide the unexpected value when boot mode changes.
4. Updated SATA RAID OPROM/EFI driver to RSTe PreOS v6.0.0.1024.
5. Set PCIe correctable and uncorrectable (non-fatal) error report to disabled by default.
6. Added support for RFC4122 UUID format feature to set RFC4122 encoding from build time produced by IPMICFG 1.29 tool 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 2933 to memory POR.
10. Added support for Linux built-in utility efibootmgr.
11. Updated valid range of IPMI setup item VLAN ID to 1-4094.
12. Added driver health warning message.
13. Set NVDIMM ADR timeout to 600µs.
14. Prevented inability to flash BIOS by AFU or SUM in-band when JPME2 CMOS value is not excepted.
15. Added a help/reminder message to appear when user incorrectly selects "EFI" for "Onboard Video Option ROM" but boots to legacy.
16. 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.
17. Added support for Cascade Lake CPU.
18. Updated to SPS 4.0.04.381 or above for INTEL-SA-00213 Security Advisory.
19. Applied workaround for inability of SUM to get full setting of IODC setup item.
20. Fixed problem of setup item "Quiet Boot" staying enabled after flashing BIOS with "Quiet Boot" disabled.
21. Added workaround for failure of BIOS flash with 156 bytes PubKey (Error: "Secure Flash Rom Verify Fail").
22. Modified UEFI network description to IPv4/IPv6 to follow Industry Standard.
23. Patched problem of system hanging at 0x94 when plugging in Nvidia Tesla T4 card.
24. Fixed incorrect display of the TDP of Intel Speed Select table.

2.2 (12/6/2018)

1. First Release