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-PS**
Release Version	**3.8a SPS: 4.1.04.804**
Build Date	**10/28/2022**
Previous Version	**3.5**
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. The event log page displayed the incorrect DIMM location.** **6. The string name was changed from SMCI to Supermicro.** **7. "Vendor Keys" has been removed from the security page.** **8. a.) SMM buffer validation has been improved 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. The allocated buffer was changed from EfiBootServicesData to EfiRuntimeServicesData.** **12. Since the product does not use the Intel IE function, the MROM1 device has been disabled.**
New features	**N/A**
Fixes	**Fixed the following issues:** **1. IScsi SUPPORT has been enabled on the Purley generation.**

Release Notes from Previous Release(s)

3.5 (06/10/2021)

1. Updated RC 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-2020-2358 (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, 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 IPMI UEFI PXE boot support to all LAN port features.
6. Updated SATA/sSATA EFI driver to VROC PreOS v7.5.0.1152.
7. Fixed an issue with system not booting into PXE with DVD installed.
8. Updated Intel Server Platform Services for Purley Refresh Server Platforms HF 4 PLR 4.1.4.450.
9. Supported IPv6 HTTP Boot function.
10. Corrected a typo in "PCIe PLL SSC" setup item help string.
11. Removed Intel LAN memory 4G limit if boot mode is not legacy.
12. Updated AEP FW to FW_1.2.0.5446, uEFI driver to 3515 for IPU2021.1.

13. Added sync IPv6 status detection rule with BMC to make sure the IPv6 status is the same in BIOS and BMC web.
14. Fixed an issue due to which the "Configuration Address Source" always showed up as "DHCP" on the IPMI IPv6 page.
15. Fixed UEFI OS boot option name shows incorrectly in BIOS setup.

3.4 (10/31/2020)

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 failure of "UEFI Compliant - Boot from iSCSI peripheral" in UEFI SCT test.
16. Fixed problem of system hanging during BIOS flash if Watch Dog function is enabled.
17. Fixed inability of 6240R and some refresh 4 serial CPU frequencies to reach maximum when enabling Mwait.
18. Corrected BMC firmware revision in BIOS Setup.
19. Fixed problem of system hanging at 0xB2 with some NVMe devices.
20. Fixed problem of system hanging at POST code 0xA0 or 0xA2 when using unsupported security NVMe device and installing Hyper-V with Windows 2019.
21. Fixed inconsistency of X-AMI ID of Setup Item "Refresh Watermarks".

3.3 (02/27/2020)

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. Added support for AEP DIMMs firmware update through IPMI.
10. Updated SATA RAID OPROM/EFI driver to VROC PreOS v6.3.0.1005.
11. Implemented dynamic update of OCP setting for 165W CPU to patch hardware limitation of system rebooting unexpectedly during CPU stress test.
12. Fixed mismatch of Secure Boot Mode value.
13. Removed requirement to use Admin password for erasing TCG device.
14. Fixed problem of two CentOS boot items occurring in boot order if CentOS is installed in RAID 1 system.
15. Fixed failure of JBOF device detection.

3.2a (2/14/2020)

1. Changed BIOS revision to 3.2a.
2. Fixed problem of system hanging or rebooting at ready to boot when system has AOC-MTG-I4SM-O, AOC-STGF-I2S-O, BPN-ADP-S3008L-L6IP, and SMC SATADOM.

3.2 (10/30/2019)

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 for INTEL-SA-00241 Security Advisory to address CVE-2019-11090, CVE-2019-11088, CVE-2019-0165, CVE-2019-0166, CVE-2019-0168, CVE-2019-0169, CVE-2019-11086, CVE-2019-11087, CVE-2019-11101, CVE-2019-11100, CVE-2019-11102, CVE-2019-11103, CVE-2019-11104, CVE-2019-11105, CVE-2019-11106, CVE-2019-11107, CVE-2019-11108, CVE-2019-11110, CVE-2019-11097, CVE-2019-0131, CVE-2019-11109, CVE-2019-11131, CVE-2019-11132, and CVE-2019-11147 security issues.
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. Displayed CPU Flex Ratio-related setup items when the CPU on system supports IntelR Speed Select technology "Performance Profile" feature.
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. Updated the behavior for the feature that updates SMBIOS Type 1 and 3 with FRU0.
10. Updated VBIOS and VGA EFI Driver to 1.10.
11. Added recommended AEP DIMM firmware version.
12. Disabled ADDDC/SDDC and set PPR as hPPR.
13. Moved code for masking Mwait instruction to end of POST.
14. Enhanced F12 hot key PXE boot feature.
15. Fixed mismatch of Secure Boot value.
16. Implemented dynamic change for Secure Boot Mode default value.

17. Added support for keeping Linux MOK keys database.
18. Added Redfish/SUM Secure Boot feature and updated OOB for secure boot and reserve Key.
19. Updated iSATA port 4 and port 5 TX/RX settings.
20. Added Enhanced PPR function and set disabled as default.
21. Corrected display of the IPMI AUX revision.
22. Corrected sequence of Boot Order.
23. Fixed problem of two OS (Redhat & Ubuntu) boot devices appearing in boot order.
24. Fixed inability to preserve Linux secureboot keys after InBand BIOS update in Linux OS.
25. Fixed problem of key details showing "Security Violation" after loading Factory secure boot keys.

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 inability to change IPv6 address or IPv6 Router1 IP address.
9. Corrected DMI table type 41 number when installing different types of SIOM add-on cards.

3.0c (3/30/2019)

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. Set PCIe correctable and uncorrectable (non-fatal) error report to disabled by default.
5. Disabled unused SPS ME "CUPS IIO" and "Volumetric Airflow" sensor.
6. Added support for Linux built-in utility efibootmgr.
7. Updated valid range of IPMI setup item VLAN ID to 1-4094.
8. Enhanced BIOS setup menu to auto-switch the Option ROM's value and hide the unexpected value when boot mode changes.
9. 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.
10. Changed OPROM settings to EFI to correct behavior of the OEM BIOS with the boot mode changed to UEFI without other changes.
11. Set SDDC+1/ADDDC to enabled by default.
12. Fixed failure of CPU PBF (Prioritized Base Frequency).
13. Added workaround for failure of BIOS flash with 156 bytes PubKey (Error: "Secure Flash Rom Verify Fail").
14. Modified UEFI network description to IPv4/IPv6 to follow Industry Standard.
15. Fixed malfunction of AOC-MTG-i2T SIOM sensor and OPROM control.
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. Added support for Monitor Mwait feature.
4. Patched missing PSU information if backplane MCU reports wrong PSU information.
5. Added SIOM add-on card back to SMBIOS Type 41 to handle Linux OS network configuration case.
6. Set BMC MAC address to UUID for system without onboard LAN1 or with onboard LAN1 disabled.
7. Hid setup item "L2 RFO Prefetch Disable" to adhere to draft template v0.7.
8. Changed BIOS revision to 3.0a.
9. Enabled RFC4122 UUID support.
10. Fixed malfunction of disabling Watch Dog while flashing BIOS under OS.
11. Fixed problem of BIOS always retrying boot when Re-Try Boot is Disabled.
12. Fixed malfunction of support for LEGACY to EFI.
13. Fixed failure of always turbo in new Linux kernel 7.x.
14. Fixed problem of system hanging and falling into a dead loop when setting enabled CPU core number to 1 in always turbo mode.
15. Fixed problem of CPU core numbers and maximum turbo ratio not matching in always turbo mode.
16. Fixed failure of CPU PBF (Prioritized Base Frequency).

2.1 (8/23/2018)

1. Updated CPU microcode to address 'Spectre' derivatives (CVE-2018-3639 & CVE-2018-3640) security issue.
2. Changed BIOS revision to 2.1.
3. Updated Giga LAN EFI driver 8.3.0.4 (IBA 23.1).
4. Added 1T option for MMIO High Base setup item.
5. Added BIOS/ME downgrade check for SPS 4.0.4.381.
6. Changed maximum speed in SMBIOS type 4 to 4500Mhz.
7. Added one event log to record that the event log is full.
8. Added support for SATA FLR.
9. Displayed PPR setup item.
10. Added a patch to prevent reboot hang when installing AVAL APX-3224 card.
11. Moved SIOM SMBIOS definition from type 41 to type 9.
12. Exported driver health menu under setup.
13. Added support for full function of AOC-MHIBE-M1CGM SIOM.
14. Fixed problem of Ctrl + Alt + Del causing system to hang after flashing BIOS.
15. Fixed problem of some NVDIMM items not appearing in setup menu.
16. Fixed incorrect VPD data and oversized string to prevent system from hanging.
17. Fixed problem of system hanging when installing Linux OS after COM1 & COM2 IO/IRQ exchange.
18. Fixed problem of SUM GetSataInfo showing incorrect "Configuration Type" when setting "Configure sSATA as" to "AHCI" or "RAID" on sSATA controller.
19. Fixed issue with IPMI firmware to enable storage card to show temperature.

2.0b (2/24/2018)

1. Updated CPU microcode to address CVE-2017-5715 security patch issue.
2. Updated Purley RC 151.R03.
3. Changed RC default setting to upgrade POST Memory correctable error to uncorrectable error and map out the channel.
4. Patched for inability of AOC-MH25G-b2S2G to show sensor.

5. Disabled CPU2 IIO PCIe root port ACPI hot plug function.
6. Fixed inability of AOC-MTG-i4T to show sensor.
7. Fixed problem of SMC skipping first boot option in UEFI mode when retrying boot.
8. Fixed inability to reset the system under DOS by pressing "Ctrl-Alt-Del" on USB keyboard when "Port 60/64 Emulation" is disabled.
9. Fixed inability of some CPUs to display correct microcode revision under BIOS setup menu.

2.0 (11/30/2017)

1. Changed BIOS revision to 2.0.
2. Updated Purley RC 149.R09, SPS 4.0.04.294, ACM files, and CPU microcode.
3. Set message "BIOS cannot support downgrade to previous version or ROMID mismatch" to show when trying to downgrade BIOS or flash other model of BIOS.
4. Fixed problem of serial console output showing SMC logo when EarlyVideo logo item is disabled.
5. Fixed problem of the Last UCE report (mapout) DIMM sometimes not matching real UCE DIMM location.
6. Fixed problem of IPMI SEL logging "Memory training failure." and "No memory DIMM detected, install memory DIMMs." twice per reboot.
7. Fixed problem of TPM 1.2 PS index not being Write-Protected so that the content of TPM 1.2 PS index still can be modified after TPM 1.2 is nvLocked.
8. Fixed problem of changes to CPU core Enable/Disable in setup menu sometimes not taking effect on Windows OS.
9. Fixed problem of system hanging during BIOS flashing if Watch Dog function is enabled.
10. Fixed system reboots endlessly when equipping dTPM module.
11. Fixed inability of DMI Customized Information to preserve after user implements BIOSLoadDefault or CMOS Clear Action.