BIOS Release Notes

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	**B11DPT**
Release Version	**4.0**
Build Date	**09/20/2023**
Previous Version	**3.4**
Update Category	**Recommended**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Changed BIOS revision to 4.0.** **2. Updated AMI label 5.14_PurleyCrb_0ACLA060 for RC0628.P50 IPU 2023.3.** **a. 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.** **b. For INTEL-SA-00828 Security Advisory to address CVE-2022-40982 (6.5, Medium) security issue.** **3. Updated Cascade Lake-SP CPU PV microcode for IPU.** **4. Updated Intel Server Platform Services for Purley Refresh Server Platforms IPU2023.3 4.1.5.2.**
New features	**None**
Fixes	**None**

Release Notes from Previous Release(s)

3.4 (2/17/2021)

1. Changed BIOS version to 3.4.
2. 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), and 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.
3. Updated Skylake-SP/Cascade Lake-SP CPU PV microcode from IPU 2020.2 PV 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).
4. 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.
5. Updated Intel BIOS ACM firmware to v1.7.41 (20200406) and SINIT ACM Firmware to v1.7.49 (20200406).

3.1a (9/6/2019)

1. Reverted label update to previous stable version (WW16).
2. Updated BIOS version to 3.1a.
3. Displayed third revision number for IPMI Firmware.
4. Updated for dynamic AEP power.
5. Updated for onboard LAN port.
6. Updated to latest microcode.
7. Fixed problem of F12 PXE boot causing DMI data to return to default value.
8. Fixed failure of UEFI iSCSI OS installation.

3.1 (5/29/2019)

1. Changed BIOS version to 3.1.
2. Updated the Leaky Bucket to 2.15 minutes at 2666MHz.
3. Set SDDC+1 to disabled by default.
4. Updated Intel RSTe to 6.1.0.1017.
5. Updated Intel RC to ww16.
6. Updated Hyper Threading and VMC default settings.
7. Updated memory error log fru_text.
8. Updated the Memory Correctable Threshold to 512.
9. Set ADDDC/SDDC to enabled by default.
10. Set PCIe hot plug to enabled by default.
11. Updated LAN firmware to version 3.45.
12. Updated extended type 17.
13. Merged 16 records of DMI type to a single record.
14. Updated NVDIMM ADR timer to 600us.
15. Updated VRM.

2.0c (7/30/2018)

1. Updated CPU microcode to address 'Spectre' derivatives (CVE-2018-3639 & CVE-2018-3640) security issue.

2. Changed BIOS revision to 2.0c.
3. Added bifurcation and slot configuration for Mezzanine and FrontIO Cards.
4. Enabled the Jumperless BIOS Flash feature.
5. Updated for VMD mode support.
6. Updated Intel microcode to 0x4D.
7. Added Jumperless solution.
8. Added delay For iSCSI Initialized.
9. Fixed problem of NVMe ejection function not working using AOM-BPNIO-SNE.
10. Fixed failure to recognize the U.2 device on Intel VMD.
11. Fixed failure of NVMe ejection function.
12. Fixed incorrect maximum power reading in CMM.
13. Fixed a BIOS build issue in 7/26 BIOS.
14. Fixed failure of LoadDefaultBiosCfg in SUM ATT cases TC210 and TC304.

2.0b (2/21/2018)

1. Updated Intel microcode to 0x43 to address Intel side-channel security problem.
2. Changed revision to 2.0b.
3. Changed SMBIOS type 16 number of memory device to 6.
4. Added delay after issuing S5 command to solve problem of MSMI being triggered when power is turned off.
5. Fixed problem of DMI data being erased during SUM testing.

2.0a (12/7/2017)

1. Updated ME firmware to 2.88 to fix Intel security issue.
2. Remapped PCIE NVMe VPP.
3. Enabled NVMe UEFI driver by default.
4. Changed number of memory in BIOS setup.
5. Updated Intel Microcode to 3A for security patch.
6. Changed revision to 2.0a.
7. Fixed problem of LSI3108 OPROM becoming disabled when boot order is changed.
8. Fixed problem of IPMI displaying incorrect onboard NIC MAC address.
9. Fixed problem of DMI data being erased during SUM testing.

Product Manager *Date*