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	**X11DPU-ZE+**
Release Version	**3.8b SPS: 4.1.04.901**
Build Date	**01/06/2023**
Previous Version	**3.6**
Update Category	**Recommended**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Changed BIOS revision to 3.8b.** **2. Updated AMI label 5.14_PurleyCrb_0ACLA058 for RC0626.P01 IPU 2023.1.** **a) For INTEL-SA-00717 Security Advisory to address CVE-2022-32231 (7.5, High) / CVE-2022-26343 (8.2, High) security issues.** **3. Updated token RC_VERSION_VALUE setting to 626.P01.** **4. 4. Updated Cascade Lake-SP CPU PV microcode for IPU 2023.1.**
New features	**None**
Fixes	**None**

Release Notes from Previous Release(s)

3.6 (1/18/2022)

1. *Change BIOS revision to 3.6.*
2. *Update SATA/sSATA EFI driver to VROC PreOS v7.7.0.1054.*
3. *Update AEP uEFI driver to 1.0.0.3531 for IPU2021.2.*
4. *Update AMI label 5.14_PurleyCrb_0ACLA054 for RC0616.D08 2021.2 IPU.*
5. *Updated Intel Server Platform Services for Purley Refresh Server Platforms IPU2021.2 HF1 4.1.4.654.*
6. *Update BIOS ACM 1.7.51, SINIT ACM 1.7.51 PW.*
7. *Updated Skylake-SP/Cascade Lake-SP CPU PV microcode*.

3.5 (6/2/2021)

1. Updated RC 612.D02 and IPU 2021.1 PV 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 v7.6.0.1012.
7. Enabled system to boot into PXE with DVD installed.
8. Added support for IPv6 HTTP Boot function.
9. Corrected typo in "PCIe PLL SSC" setup item help string.
10. Removed 4G limit of Intel LAN memory if boot mode is not legacy.
11. Synced IPv6 status detection rule with BMC to make sure IPv6 status is the same in BIOS and BMC web.
12. Fixed problem of "Configuration Address Source" always showing "DHCP" on IPMI IPv6 page.
13. Corrected display of UEFI OS boot option name in BIOS setup.

3.4 (11/4/2020)

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. Corrected "Station MAC Address" display order when "Configuration Address Source" is set to "Static".
10. Added PPR success result SEL and set duplicated PPR SELs to be filtered out if the location is same.
11. 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".
12. 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).
13. Fixed problem of EFI version of PassMark MemTest86 hanging when SMCI Redfish Host Interface is not supported in IPMI firmware.
14. Fixed failure of "UEFI Compliant - Boot from iSCSI peripheral" in UEFI SCT test.
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.
20. Fixed inconsistency of X-AMI ID of Setup Item "Refresh Watermarks".

3.3 (02/24/2020)

1. Updated BIOS ACM to 1.7.40 and SINIT ACM to 1.7.48 PW.
2. Updated Skylake-SP/Cascade Lake-SP CPU microcode for Intel-SA-00329 (CVE2020-0548 2.8 Low, 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 BIOS item “HDD password prompt Control” to allow enabling or disabling HDD password prompt during POST.
6. Enabled UPI correctable error logging in BIOS event log and IPMI SEL.
7. Enabled HTTP/HTTPS booting even when USB UNDI module is enabled.
8. Updated BIOS to show the second IIO device when a x8 slot is split into x4x4.

3.2 (10/22/2019)

1. Updated AMI label 5.14_PurleyCrb_0ACLA049_BETA for BKC WW36 RC595.D04 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 2019for 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. Updated SATA/sSATA RAID OPROM/EFI driver to VROC PreOS v6.2.0.1034.
20. Disabled ADDDC/SDDC and set PPR as hPPR.
21. Updated RC595.D04 hot fix.
22. Added Enhanced PPR function.
23. Removed PXE option for "OnBoard LanX Option ROM" when "Boot mode select" is UEFI.
24. Fixed inability of InBand Update BIOS in Linux OS to preserve Linux secureboot keys.
25. Corrected display of the IPMI AUX revision.
26. Fixed problem of boot time increasing by more than two minutes per boot after running stress over hundreds of cycles.
27. Fixed inability to identify duplicated NVMe boot option with more than one of the same NVMe drives on an add-on card.
28. Changed OOB download and Upload Bios Configuration sequence.
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).