

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	X11DPG-OT-CPU
Release Version	3.8b SPS: 04.01.04.901
Release Date	1/17/2023
Previous Version	3.8a
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 0626.P01. 4. Updated Cascade Lake-SP CPU PV microcode for IPU 2023.1. 5. Updated VROC SATA/sATA EFI driver to VROC PreOS v7.8.0.1012.
New features	None
Fixes	None

Release Notes from Previous Release(s)

3.8a (10/31/2022)

1. Updated AMI label 5.14_PurleyCrb_OACLA057 for RC0623.D09 2022.3 IPU to address INTEL-SA-00688. CVE-2022-26343 (8.2 High).
2. Updated AEP uEFI driver to 01.00.00.3536 for IPU2022.3.
3. Updated Skylake-SP/Cascade Lake-SP CPU PC microcode for IPU 2022.2.
4. Updated token RC_VERSION_VALUE setting to 622.D07.
5. Modified String naming from SMCI to Supermicro.
6. 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).

3.6a (05/06/2022)

1. Changed BIOS Revision to 3.6a.
2. Fixed LAN EEPROM DPGOT2A.ZIP, tools cannot offline update LAN2 issue.

3.6 (1/25/2022)

1. Change BIOS Revision to 3.6.
2. Updated 5.14_PurleyCrb_OACLA054 for RC update and 2021.2 IPU PV.
3. Updated Skylake-SP H0/M0/U0 stepping CPU PC microcode 02006C0A, Cascade Lake-SP B0 stepping CPU PC microcode 0400320A, Cascade Lake-SP B1 stepping CPU PC microcode 0500320A.
4. Updated to SPS 04.01.04.601.
5. Updated Intel BIOS ACM Firmware to v1.7.51 and SINIT ACM Firmware to v1.7.51.

3.4 (12/18/2020)

1. Changed BIOS Revision to 3.4.
2. Updated 5.14_PurleyCrb_OACLA052 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.
3. 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).
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).

3.3a (8/13/2020)

1. Changed BIOS revision to 3.3a.
2. Removed extreme performance.

3.3 (2/21/2020)

1. *Changed BIOS revision to 3.3.*
2. *Updated Intel Server Platform Services 4.1.4.381 for Purley-Refresh Platforms.*
3. *Updated Intel Reference Code to IPU2020.1 Rev: RC0602.D02.*
4. *Updated Intel BIOS ACM firmware to v1.7.40 (20190909) and SINIT ACM firmware to v1.7.48 (20191029).*
5. *Added SMC HDD Security feature.*
6. *Updated Skylake-SP/Cascade Lake-SP CPU microcode from Intel-Restricted-2020-1-IPU limit beta for INTEL-SA-00317 Security Advisory to address CVE-2019-14607 (5.3, Medium) security issue and for INTEL-SA-00289 Security Advisory to address CVE-2019-11157 (7.9, High) security issue.*
7. *Added support for Driver Health.*
8. *Patched problem of system hanging at 94 with new NVidia RTX 6000/8000.*

3.2a 12/11/2019

1. *Updated BIOS version to 3.2a.*
2. *Fixed malfunction of LAN after using programmer to update the BIOS.*

3.2 (11/7/2019)

1. *Updated BIOS version to 3.2.*
2. *Updated Intel Skylake-SP H0 Microcode to 02000065.*
3. *Updated Intel Cascadelake-SP B0 Microcode to 0400002C.*
4. *Updated Intel Cascadelake-SP B1 Microcode to 0500002C.*
5. *Updated Intel Server Platform Services 04.01.04.339.0 for Purley-Refresh Platforms.*
6. *Displayed third revision number for IPMI Firmware.*
7. *Updated Intel BIOS ACM Firmware to v1.7.3 (20190712) and SINIT ACM Firmware to v1.7.45 (20190710).*
8. *Updated Intel Reference Code to BKC WW36 Rev: RC0595.D04.*
9. *Disabled ADDDC/SDDC and set PPR as hPPR.*
10. *Added support for VMD for onboard NVMe.*
11. *Fixed problem of F12 PXE boot causing DMI data to return to default value.*

3.1 (04/30/2019)

1. *Changed BIOS revision to 3.1.*
2. *Updated Intel Reference Code to BKC WW16 Rev: RC0584.D01.*
3. *Updated Intel Xeon microcode for Skylake-EP to Rev. 5E for Intel Xeon Skylake-EP H0/H0-QS.*
4. *Added Cascade Lake Server B0 Stepping CPU Support with Rev. 24 for Intel Xeon Scalable Cascade Lake Server B0-QS.*
5. *Added Cascade Lake Server B1 Stepping CPU Support with Rev. 24 for Intel Xeon Scalable Cascade Lake Server B1-QS.*
6. *Updated Intel Server Platform Services 04.01.04.296.0 for Purley-Refresh Platforms.*
7. *Updated RSTe VMD/SATA/sSATA driver to v6.1.0.1017.*
8. *Set RAS Feature SDDC+1 to disabled by default.*

3.0c (4/9/2019)

1. *Changed BIOS revision to 3.0c.*
2. *Updated Intel Reference Code to BKC 2019_WW12 Rev: RC0580.D04.*
3. *Set SDDC+1/ADDDC to enabled by default.*
4. *Temporarily fixed error for SKX (CLX) 4114 CPU memory training with Micron (18ASF2G72PDZ-2G6E1) RDIMM.*

3.0b SPS: 04.01.04.256.0 (3/13/2019)

1. *Changed BIOS revision to 3.0b.*
2. *Updated Intel Reference Code to BKC 2019_WW10 Rev: RC0578.D07.*
3. *Updated Intel Xeon microcode for Skylake-EP to Rev. 5a for Intel Xeon Skylake-EP H0/H0-QS.*
4. *Added Cascade Lake Server A0 Stepping CPU Support with Rev. 10 for Intel Xeon Scalable Cascade Lake Server A0-QS.*
5. *Added Cascade Lake Server B0 Stepping CPU Support with Rev. 21 for Intel Xeon Scalable Cascade Lake Server B0-QS.*
6. *Added Cascade Lake Server B1 Stepping CPU Support with Rev. 21 for Intel Xeon Scalable Cascade Lake Server B1-QS.*
7. *Updated Intel Server Platform Services 04.01.04.256.0 for Purley-Refresh Platforms.*
8. *Updated Intel BIOS ACM firmware to v1.7.0 and SINIT ACM firmware to v1.7.1.*
9. *Fixed inability to update BIOS by AFU tool.*

3.0a (2/26/2019)

1. *Added support for Purley Refresh platform.*
2. *Changed BIOS revision to 3.0a.*
3. *Updated Intel Reference Code to BKC 2019_WW06 Rev. RC0575.D01.*
4. *Updated Intel Xeon microcode for Skylake-EP to Rev. 5a for Intel Xeon Skylake-EP H0/H0-QS.*
5. *Updated Intel Server Platform Services 04.01.04.251.0 for Purley-Refresh Platforms.*
6. *Updated Intel BIOS ACM firmware to v1.7.0 and SINIT ACM firmware to v1.7.1.*
7. *Increased ADR timeout to 600us for NVDIMM.*
8. *Updated redriver setting on X10 PCIe board slots 6 & 7 according to hardware requirement.*

2.1a (10/02/2018)

1. *Changed BIOS revision to 2.1a.*
2. *Added support for the X11DPG-O-PCIe board.*
3. *Changed MMIO High Granularity size from 256G to 1024G to fix problem of hang 91 occurring with 8x V100 GPU.*

2.1 (9/17/2018)

1. Updated CPU microcode to address 'Spectre' derivatives (CVE-2018-3639 & CVE-2018-3640) security issue.
2. Changed BIOS revision to 2.1.
3. Added code to program CPLD for backplane detection.
4. Updated Intel code to correct issue with NVIDIA P2P bandwidth.
5. Fixed inability to execute UEFI PXE boot with AOC-MGP-i2 and added i350 UEFI Option ROM for X11DPG-SN.
6. Fixed failures of Test Case 220 and 308 Test.

2.0b (2/26/2018)

1. Implemented enhancement to address 'Spectre' variant 2 (CVE 2017-5715) security patch issue.
2. Updated BIOS version to 2.0b.
3. Added support for IPMI to fix RSC-G2F-A66-X1 sensor reading.
4. Added 2U PLX riser card to support list.
5. Fixed failure of SIOM sensor reading.
6. Fixed failure of IOBP Check.

Product Manager

Date