BIOS Release Notes Form

Product Name	**X11DPi-N(T)**
Release Version	**3.8a SPS: 04.01.04.804**
Build Date	**10/27/2022**
Previous Version	**3.6**
Update Category	**Recommended**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Changed BIOS Revision to 3.8a.** **2. Updated AMI label 5.14_PurleyCrb_0ACLA057 for RC0623.D09 2022.3 IPU to address INTEL-SA-00688. CVE-2022-26343 (8.2 High).** **3. Updated AEP uEFI driver to 01.00.00.3536 for IPU2022.3.** **4. Updated Skylake-SP/Cascade Lake-SP CPU PC microcode for IPU 2022.2.** **5. Modify String naming from SMCI to Supermicro.** **6. Updated BIOS ACM Firmware v1.7.54 and SINIT ACM Firmware v1.7.55 PW for IPU2022.1 to address.** **7. Updated AEP uEFI driver to 01.00.00.3534 for IPU2022.2.**
New features	**N/A**
Fixes	**N/A**

Release Notes from Previous Release(s)

3.6 (01/25/2022)

1. Changed BIOS Revision to 3.6.
2. Updated 5.14_PurleyCrb_0ACLA054 with RC update and 2021.2 IPU PV.
3. Updated Skylake-SP/Cascade Lake-SP CPU PC microcode from IPU2021.2
4. Updated SPS to 04.01.04.601.
5. Update Intel BIOS ACM Firmware to v1.7.51 and SINIT ACM Firmware to v1.7.51.
6. Disabled Intel Boot Guard which was enabled in BIOS_X11DPi-N-0917_20211229_3.6_STD.bin.
7. Fixed ATT BIOS ECO TC 113 failure.

3.5 (06/29/2021)

1. Changed BIOS revision to 3.5.
2. Updated 5.14_PurleyCrb_0ACLA053 for RC update and 2021.1 IPU PV.
3. Updated Skylake-SP/Cascade Lake-SP CPU PC microcode from IPU2021.1.
4. Updated SPS 04.01.04.505.
5. Updated Intel BIOS ACM Firmware to v1.7.43 (20201216) and SINIT ACM Firmware to v1.7.4A (20201216).

3.4 (11/23/2020)

1. Changed BIOS Revision 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), 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).
6. Fixed failure of ATT BIOSECO TC#220.

3.3a (9/18/2020)

1. Changed BIOS revision to 3.3a.
2. Updated Skylake-SP/Cascade Lake-SP CPU microcode from Intel-Restricted-2020-1-IPU.
3. Fixed inability of BIOS to load default when plugging in M.2.
4. Fixed problem of DVM-LITE-DVD18-HBT causing the system to keep rebooting.
5. Fixed problem of Micron NVMe U.2 displaying ???? in BIOS boot options when there is also an M.2 installed on the system.
6. Allowed HTTP URI for HTTP boot.

3.3 (2/24/2020)

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. Enhanced PPR log function.
9. Added support for HDD erase and set password function when using SUM.

3.1a (10/16/2019)

1. Updated BIOS version to 3.1a.
2. Displayed third revision number for IPMI Firmware.
3. Updated Intel Skylake-SP H0 Microcode to 02000065.
4. Updated Intel Cascadelake-SP B0 Microcode to 0400002C.
5. Updated Intel Cascadelake-SP B1 Microcode to 0500002C.
6. Updated Intel Server Platform Services 04.01.04.339.0 for Purley-Refresh Platforms.
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 Enhanced PPR function and set disabled as default.
11. Fixed problem of F12 PXE boot causing DMI data to return to default value.

3.1 (04/26/2019)

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 SDDC Plus One or SDDC to disabled by default.

3.0c (4/1/2019)

1. Changed BIOS revision to 3.0c.
2. Updated Intel Reference Code to BKC 2019_WW12 Rev: RC0580.D04.
3. Updated Intel Xeon microcode for Skylake-EP to Rev. 5A for Intel Xeon Skylake-EP H0/H0-QS.
4. Added Cascade Lake Server B0 Stepping CPU Support with Rev. 21 for Intel Xeon Scalable Cascade Lake Server B0-QS.
5. Added Cascade Lake Server B1 Stepping CPU Support with Rev. 21 for Intel Xeon Scalable Cascade Lake Server B1-QS.
6. Updated Intel Server Platform Services 04.01.04.256.0 for Purley-Refresh Platforms.
7. Updated Intel BIOS ACM firmware to v1.7.1 and SINIT ACM firmware to v1.7.2.
8. Updated SMBIOS Types 16 and 17 for DCPMM support.

9. Set SDDC+1/ADDDC to enabled by default.
10. Fixed problem of SKX/CLX 4xxx SKU CPU causing memory training error with Micron RDIMM (18ASF2G72PDZ-2G6E1).
11. Fixed malfunction of hotkey F12 when switching onboard LAN Option ROM to EFI.

3.0a (1/11/2019)

1. Added support for Purley Refresh platform.
2. Changed BIOS revision to 3.0a.
3. Updated Intel Reference Code to BKC WW52 Rev: RC0566.D03.
4. Updated Intel Xeon microcode for Skylake-EP to Rev. 57 for Intel Xeon Skylake-EP H0/H0-QS.
5. Updated Intel BIOS ACM firmware to v1.7.0 and SINIT ACM firmware to v1.7.1.
6. Updated RSTe VMD/SATA/sSATA driver to v6.0.0.1024.
7. Enabled RFC4122 UUID support.
8. Updated BIOS Setup Template to v0.7.
9. Fixed malfunction of Intel SST-BF feature.

2.1 (6/29/2018)

1. Updated CPU microcode to address 'Spectre' derivatives (CVE-2018-3639 & CVE-2018-3640) security issue.
2. Changed BIOS revision to 2.1.
3. Enabled the Jumperless BIOS Flash feature.
4. Fixed certain SUM-related issues on Project Board.
5. Set Descriptor Region of BIOS Region Write Access to "No".

2.0b (2/28/2018)

1. Implemented enhancement to address 'Spectre' variant 2 (CVE 2017-5715) security patch issue.
2. Changed BIOS revision to 2.0b.
3. Added maximum performance option under Energy Performance on BIOS setup page.
4. Removed BIOS time stamp from main BIOS setup page.
5. Prevented certain corner cases that cause ME update to fail when using AFUEFI tool.
6. Fixed inability of certain SKX CPUs to display the microcode version correctly on BIOS setup page.
7. Fixed inability to use OOB SUM to get current BIOS configuration file.
8. Fixed problem of system hanging at POST code "91" after BIOS update with EFI shell command "reset".