BIOS Release Notes

Product Name	**X11OPI**
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 2023.3.** **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 (10/26/2020)

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 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).
6. Added support for SIOM AOC-M25G-M4S.

3.3 (3/9/2020)

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. Downgraded memory Patrol Scrubbing UC errors to correctable errors.
6. Updated RSTe VMD/SATA/sSATA driver to v6.2.0.1034.
7. Updated Intel Xeon microcode for Skylake-EP.
8. Added Cascade Lake Server B0 Stepping CPU Support.
9. Added Cascade Lake Server B1 Stepping CPU Support.
10. Added SMC HDD Security feature.
11. Added support for Driver Health.
12. Enhanced PPR log function.

3.2 (12/3/2019)

1. Changed BIOS revision to 3.2.
2. Updated Intel Reference Code to BKC WW36 Rev: RC0595.D04.
3. Updated Intel Xeon microcode for Skylake-EP to Rev. 65 for Intel Xeon Skylake-EP H0/H0-QS.
4. Added Cascade Lake Server A0 Stepping CPU Support with Rev. 12 for Intel Xeon Scalable Cascade Lake Server A0-QS.
5. Added Cascade Lake Server B0 Stepping CPU Support with Rev. 2C for Intel Xeon Scalable Cascade Lake Server B0-QS.
6. Added Cascade Lake Server B0 Stepping CPU Support with Rev. 2C for Intel Xeon Scalable Cascade Lake Server B1-QS.
7. Updated ME firmware revision to SPS E5 04.01.04.339.0. 8. Displayed third revision number for IPMI Firmware.
9. Fixed issue with Redfish API boot order change.
10. Disabled ADDDC/SDDC and set PPR as hPPR.
11. Added Enhanced PPR function and set disabled as default.
12. Fixed problem of F12 PXE boot causing DMI data to return to default value.

3.1 (5/10/2019)

1. Updated Intel Reference Code to BKC WW12 Rev: RC0584.D01.
2. Updated Intel Xeon microcode for Skylake-EP to Rev. 5E for Intel Xeon Skylake-EP H0/H0-QS.
3. Added Cascade Lake Server A0 Stepping CPU Support with Rev. 10 for Intel Xeon Scalable Cascade Lake Server A0-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 B0 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 Intel BIOS ACM firmware to v1.7.1 and SINIT ACM firmware to v1.7.2.
8. Updated for new VRM.
9. Updated RSTe VMD/SATA/sSATA driver to v6.1.0.1017.
10. Updated for help strings. 11. Set RAS feature SDDC+1 to disabled by default, RAS feature ADDDC to enabled by default, and Leaky Bucket to 2.15 minutes with DDR speed 2666MHz. 12. Changed Memory Correctable Threshold to 512.

3.0a (02/15/2019)

1. Updated Intel Reference Code to BKC WW04 Rev: RC0571.D03.
2. Updated Intel Xeon microcode for Skylake-EP.
3. Added Purley platform refresh A0 Stepping CPU Support.
4. Added Purley platform refresh B0 Stepping CPU Support.
5. Added Purley platform refresh B1 Stepping CPU Support.
6. Updated RSTe VMD/SATA/sSATA driver to v6.0.0.1024.
7. Updated Intel Server Platform Services 04.01.04.251.0 for Purley-Refresh Platforms.
8. Updated Intel BIOS ACM Firmware to v1.7.1 and SINIT ACM Firmware to v1.7.1.
9. Enabled RFC4122 UUID support.
10. Added support for Tesla T4 GPU.
11. Updated for QPI correctable error.
12. Updated memory threshold to 512.
13. Hid WHEA errors from pROC source.
14. Updated for BMC UCE log.
15. Updated for X-AMI string and fixed SUM TC220 and TC308 failure issue.

2.1a (07/09/2018)

1. Updated Intel Management Engine firmware to address CVE-2018-3643 security issue.
2. Updated RSTe VMD/SATA/sSATA driver to v5.5.0.1028.
3. Updated for QPI correctable error.
4. Updated memory threshold to 512.
5. Hid WHEA errors from pROC source.
6. Updated for BMC UCE log.

2.1 (07/09/2018)

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

2.0b (02/23/2018)

1. Changed BIOS revision to 2.0b.
2. Updated Intel Xeon microcode for Skylake-EP. - rev. 43 for Intel Xeon Skylake-EP H0/H0-QS.
3. Updated RSTe VMD/SATA/sSATA driver to v5.4.0.1039.
4. Removed BIOS time stamp from main BIOS setup page.
5. Displayed BIOS version when doing BIOS update using IPMI Web.

_____ _____

Product Manager *Date*