BIOS Release Notes Form

Product Name	**X11QPH+**
Release Version	**4.0**
Release Date	**7/11/2023**
Previous Version	**3.9**
Update Category	**Recommended**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Updated AMI label 5.14_PurleyCrb_0ACLA060 for RC0628.P50 IPU 2023.3.** **(1). 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.** **(2). For INTEL-SA-00828 Security Advisory to address the CVE-2022-40982 (6.5, Medium) security issue.** **2. Updated Cascade Lake-SP CPU PV microcode for IPU 2023.3.** **3. Updated Intel Server Platform Services for Purley Refresh Server Platforms IPU2023.3 4.1.5.2.** **4. Updated DBX file for AMI-SA50182 Secure Boot DBX Update.** **5. Updated Intel Server Platform Services for Purley Refresh Server Platforms IPU2023.3 4.1.5.002.**
New features	**None**
Fixes	**1. Added buffer overflow security patch.**

Release Notes from Previous Release(s)

3.9(04/11/2023)

1.Change BIOS revision to 3.9.
2.Update AMI label 5.14_PurleyCrb_0ACLA059 for RC0626.P01 IPU 2023.2 (1). For INTEL-SA-00807 Security Advisory to address CVE-2022-38087(4.1, Medium) and CVE-2022-33894(7.5, High) security issues.
3.Update token RC_VERSION_VALUE setting to 0627.P11.
4.Updated Cascade Lake-SP CPU PV microcode for IPU 2023.2.

3.8b(01/13/2023)

1.Updated AMI label 5.14_PurleyCrb_0ACLA057 for RC0623.D09 2022.3 IPU to address INTEL-SA-00688. CVE-2022-26343(8.2 High) security issue.

2.Updated AEP UEFI driver to 01.00.00.3536 for IPU2022.3.

3.Updated AMI label 5.14_PurleyCrb_0ACLA058 for RC0626.P01 IPU 2023.1 (1). Updated INTEL-SA-00717 Security Advisory to address CVE-2022-32231 (7.5, High) / CVE-2022-26343 (8.2, High) security issues.

4.Updated token RC_VERSION_VALUE setting to 0626.P01.

5.Updated Cascade Lake-SP CPU PV microcode for IPU 2023.1.

6.Updated VROC SATA/sSATA EFI driver to VROC PreOS v7.8.0.1012.

3.8(09/06/2022)

1. Changed BIOS revision to 3.8.

2. Updated 5.14_PurleyCrb_0ACLA053 for RC update and 2022.1 IPU PV.

3. Updated Skylake-SP/Cascade Lake-SP CPU PC microcode from IPU2022.1.

4. Updated SPS 4.1.4.700.

5. Updated Intel BIOS ACM Firmware to v1.7.54 and SINIT ACM Firmware to v1.7.45.

6. Updated Skylake-SP/Cascade Lake-SP CPU PC microcode for IPU 2022.2. (1). For INTEL-SA-00601 Security Advisory to address CVE-2021-0154(8.2, High), CVE-2021-0153(8.2, High), CVE-2021-33123(8.2, High), CVE-2021-0190(8.2, High), CVE-2021-33122(7.9, High), CVE-2021-33060(7.8, High), CVE-2021-0189(7.5, High), CVE-2021-33124(7.5, High), CVE-2021-33103(7.5, High), CVE-2021-0159(7.4, High), CVE-2021-0188(5.3, Medium) and CVE-2021-0155(4.4, Medium) security issues. (2). For INTEL-SA-00615 Security Advisory to address CVE-2022-21123(6.1, Medium), CVE-2022-21127(5.6, Medium), CVE-2022-21125(5.5, Medium) and CVE-2022-21166(5.5, Medium) security issues. (3). For INTEL-SA-00616 Security Advisory to address CVE-2021-21131(3.3, Low) and CVE-2021-21136(2.7, Low) security issues.

7. Made the following updates:

a. Updated token RC_VERSION_VALUE setting to 622.D07

b. Updated token PRICESSO_0_UCODE_VERSION setting to 02006E05. C. Updated token

FW_SPS_VERSION setting to 4.1.4.804.

8. Updated AEP uEFI driver to 01.00.00.3534 for IPU2022.2.

3.6 (12/13/2021)

1. Changed the BIOS Revision to 3.6.
2. Added VMware Pmem Support.
3. Updated 5.14_PurleyCrb_0ACLA053 for RC update and 2021.2 IPU PV.
4. Updated Skylake-SP/Cascade Lake-SP CPU PC microcode from IPU2021.2
5. Updated SPS 4.1.4.601
6. Updated Intel BIOS ACM Firmware to v1.7.51(20210621) and SINIT ACM Firmware to v1.7.51(20210621)

3.5 (06/18/2021)

1.Change BIOS Revision to 3.5.
2.Update 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 4.1.4.505
5.Update Intel BIOS ACM Firmware to v1.7.43(20201216) and SINIT ACM Firmware to v1.7.4A(20201216).

3.4 (11/04/2020)
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).

3.3a (7/23/2020)
1. Prevented duplicate NVMe boot options.
2. Changed BIOS Revision to 3.3a.
3. Updated Skylake-SP/Cascade Lake-SP CPU microcode from Intel-Restricted-2020-1-IPU.
4. Fixed inability of BIOS to load default when plugging in M.2.
5. Fixed CentOS boot item.
6. Fixed malfunction of secure erase when using SUM.

3.3 (2/25/2020)
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. Changed patrol scrub from uncorrectable 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 support for SMC HDD Security password erase and reset.
11. Added Driver Health support.
12. Added PPR test result to the System Event Log.

3.2a (1/24/2020)
1. Changed BIOS Revision to 3.2a.
2. Updated SUM with CPU 3/4 VMD configuration.
3. Changed BIOS config XML output to fix issue with Micron devices.

3.2 (11/19/2019)
1. Changed BIOS Revision to 3.2.
2. Disabled ADDDC/SDDC and set PPR as hPPR by Intel's suggestion for memory error.
3. Keep GPP_B6 high for the reboot issue.
4. Fix for changing next boot device with ipmitool. (IssueID=103477).
5. Fix for Enhanced PPR function hang issue (IssueID=102886) .