BIOS Release Notes Form

Product Name	**X11DSC**
Release Version	**3.8a SPS: 4.1.04.804**
Build Date	**10/28/2022**
Previous Version	**3.6**
Update Category	**Recommended**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Updated AMI label 5.14_PurleyCrb_0ACLA057 for RC0623.D09 2022.3 IPU.** **a. For INTEL-TA-00610 Security Advisory to address CVE-2022-26845 (8.7 High), CVE-2022-27497(8.6 High), CVE-2022-29893 (8.1 High), CVE-2021-33159 (7.4 High), CVE-2022-29466(7.3 High), and CVE-2022-29515 (6.0 Medium) security issues.** **b. For INTEL-TA-00688 Security Advisory to address CVE-2022-26006 (8.2 High) and CVE-2022-21198(7.9 High) security issues.** **2. Updated token RC_VERSION_VALUE setting to 623.D09.** **Updated token PRICESSO_0_UCODE_VERSION setting to 02006E05.** **Updated token FW_SPS_VERSION setting to 4.1.4.804.** **3. Updated Intel DCPM UEFI driver to 1.0.0.3536.** **4. Updated Skylake-SP/Cascade Lake-SP CPU PC microcode for IPU 2022.2.** **a. 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. **b. 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.** **c. For INTEL-SA-00616 Security Advisory to address CVE-2021-21131 (3.3, Low) and CVE-2021-21136 (2.7, Low) security issues.** **5. Fixed incorrectly shown DIMM location on the event log page.** **6. Modified string name from SMCI to Supermicro.** **7. Removed "Vendor Keys" on the security page.** **8. [SMIHandlerSecurityFix]** **a. Refined SMM buffer validation in SmmSmbiosELogInitFuncs.** **b. Allocated runtime buffer to trigger ELog SMI in DxeSmmRedirFuncs.** **9. Updated BIOS ACM 1.7.54 and 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).** **10. Updated VROC SATA/sSATA legacy driver to VROC PreOS v6.3.5.1003 Hot Fix to fix 10TB or higher volume drive issue.** **11. Updated VROC SATA/sSATA EFI driver to VROC PreOS v7.8.0.1012 to address:** **a. Data Loss Exposure Due to RAID 5 TRIM Support. (Document #737276)** **b. For INTEL-TA-00692 to address CVE-2022-29919 (7.8 High), CVE-2022-30338 (6.7 Medium), CVE-2022-29508 (6.3 Medium), and CVE-2022-25976 (5.5 Medium).** **12. Modified the allocated buffer from EfiBootServicesData to EfiRuntimeServicesData.**
New features	**N/A**
Fixes	**1. Enabled IScsi_SUPPORT on Purley generation.**

Release Notes from Previous Release(s)

3.6 (1/19/2022)

1. *Changed BIOS revision to 3.6.*
2. *Updated SATA/sSATA EFI driver to VROC PreOS v7.7.0.1054.*
3. *Updated AEP uEFI driver to 1.0.0.3531 for IPU2021.2.*
4. *Updated 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. *Updated BIOS ACM 1.7.51, SINIT ACM 1.7.51 PW.*
7. *Updated Skylake-SP/Cascade Lake-SP CPU PV microcode.*

3.5 (07/20/2021)

1. Updated 612.D02 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. Updated AEP firmware to FW_1.2.0.5446 and UEFI driver to 3515 for IPU2021.1.
6. Synced IPv6 status detection rule with BMC to make sure IPv6 status is the same in BIOS and BMC web.
7. Updated SATA/sSATA EFI driver to VROC PreOS v7.6.0.1012.
8. Updated data type for LanResourceAddress.

3.4b (4/27/2021)

1. Removed Intel LAN memory 4G limit if boot mode is not legacy.
2. Updated Skylake-SP/Cascade Lake-SP CPU PC microcode from IPU2021.1.
3. Synced IPv6 status detection rule with BMC to make sure IPv6 status is the same in BIOS and BMC web.
4. Downgraded VROC version to 6.3.0.1005.
5. Corrected display of UEFI OS boot option name in BIOS setup.

3.4a (1/30/2021)

1. Updated Skylake-SP/Cascade Lake-SP CPU PV microcode from Intel-Generic-Microcode-20210125_NDA.
2. Separated SATA redriver value (2021/01/29) for 90-bay single (0x84).
3. Updated Intel Server Platform Services for Purley Refresh Server Platforms HF 4 PLR 4.1.4.450.