BIOS Release Notes Form

Product Name	**X11DPD-L/M25**
Release Version	**4.0**
Build Date	**06/20/2023**
Release Date	**10/23/2023**
Previous Version	**3.8a**
Update Category	**Critical**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1.[Enhancements] Change BIOS revision to 4.0.** **2.[Enhancements] Update 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 CVE-2022-40982(6.5, Medium) security issue.** **3.[Enhancements] Update token RC_VERSION_VALUE setting to 628.P50. Update token PRICESSO_0_UCODE_VERSION setting to 02007006. Update token PRICESSO_2_UCODE_VERSION setting to 04003604. Update token PRICESSO_3_UCODE_VERSION setting to 05003604. Update token FW_SPS_VERSION setting to 4.1.5.2.**

	4.[Enhancements] Updated Cascade Lake-SP CPU PV microcode for IPU 2023.3. **5.[Enhancements] Updated Intel Server Platform Services for Purley Refresh Server Platforms IPU2023.3 4.1.5.2** **6.[Enhancements] Update DBX file for AMI-SA50182 SecureBoot DBX Update**
New features	**N/A**
Fixes	**N/A**

Release Notes from Previous Release(s)

3.8a(4/11/2023)

1.[Enhancements] Change BIOS revision to 3.8a.
2.[Enhancements] Update SATA/sSATA EFI driver to VROC PreOS v7.7.0.1054.
3.[Enhancements] Update AEP uEFI driver to 1.0.0.3531 for IPU2021.2.
4.[Enhancements] Update AMI label 5.14_PurleyCrb_0ACLA054 for RC0616.D08 2021.2 IPU. For INTEL-SA-00527 Security Advisory to address CVE-2021-0103(8.2, High), CVE-2021-0114(7.9, High), CVE-2021-0115(7.9, High), CVE-2021-0116(7.9, High), CVE-2021-0117(7.9, High), CVE-2021-0118(7.9, High), CVE-2021-0099(7.8, High), CVE-2021-0156(7.5, High), CVE-2021-0111(7.2, High), CVE-2021-0107(7.2, High), CVE-2021-0125(6.7, Medium), CVE-2021-0124(6.3, Medium), CVE-2021-0119(5.8, Medium), CVE-2021-0092(4.7, Medium), CVE-2021-0091(3.2, Low) and CVE-2021-0093(2.4, Low) security issues.
5.[Enhancements] Updated Intel Server Platform Services for Purley Refresh Server Platforms IPU2021.2 HF1 4.1.4.654.
6.[Enhancements] Update BIOS ACM 1.7.51, SINIT ACM 1.7.51 PW. For INTEL-SA-00527 Security Advisory to address CVE-2021-0103(8.2, High), CVE-2021-0114(7.9, High), CVE-2021-0115(7.9, High), CVE-2021-0116(7.9, High), CVE-2021-0117(7.9, High), CVE-2021-0118(7.9, High), CVE-2021-0099(7.8, High), CVE-2021-0156(7.5, High), CVE-2021-0111(7.2, High), CVE-2021-0107(7.2, High), CVE-2021-0125(6.7, Medium), CVE-2021-0124(6.3, Medium), CVE-2021-0119(5.8, Medium), CVE-2021-0092(4.7, Medium), CVE-2021-0091(3.2, Low) and CVE-2021-0093(2.4, Low) security issues.
7.[Enhancements] Updated Skylake-SP/Cascade Lake-SP CPU PV microcode. Updated Skylake-SP H0/M0/U0 stepping CPU PV microcode MB750654_02006C0A. Update Cascade Lake-SP B0 stepping CPU PV microcode MBF50656_0400320A. Update Cascade Lake-SP B1 stepping CPU PV microcode MBF50657_0500320A. For INTEL-SA-00532 Security Advisory to address CVE-2021-0127(5.6, Medium) security issue. For INTEL-SA-00365 Security Advisory to address CVE-2020-8673(4.7, Medium) security issue.
8.[Enhancements] Sync IPv6 status detection rule with BMC to make sure IPv6 status is the same in BIOS and BMC web.

9.[Enhancements] Update AIOM SMBIOS slot ID to meet SMC rule.
10.[Enhancements] Update AMI label 5.14_PurleyCrb_0ACLA056 for RC0622.D07 2022.2 IPU. (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.
11.[Enhancements] 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.
12.[Enhancements] Update token RC_VERSION_VALUE setting to 622.D07. Update token PRICESSO_0_UCODE_VERSION setting to 02006E05. Update token FW_SPS_VERSION setting to 4.1.4.804.
13.[Enhancements] Fix show wrong DIMM location in event log page.
14.[Enhancements] Modify String naming from SMCI to Supermicro.
15.[Enhancements] Remove "Vendor Keys" in security page.
16.[Enhancements] [SMIHandlerSecurityFix] 1.Refine SMM buffer validation in SmmSmbiosELogInitFuncs.c 2.Allocate runtime buffer to trigger ELog SMI in DxeSmmRedirFuncs.c
17.[Enhancements] Update AEP uEFI driver to 01.00.00.3534 for IPU2022.2.
18.[Enhancements] 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)
19.[Enhancements] Update VROC SATA/sSATA legacy driver to VROC PreOS v6.3.5.1003 Hot Fix to fix 10TB or higher volume drive issue.
20.[Enhancements] Update VROC SATA/sSATA EFI driver to VROC PreOS v7.8.0.1012 to address 1. Data Loss Exposure Due to RAID 5 TRIM Support. Document #737276. 2. INTEL-TA-00692. CVE-2022-29919(7.8 High), CVE-2022-30338(6.7 Medium), CVE-2022-29508(6.3 Medium), CVE-2022-25976(5.5 Medium)
21.[Fixes] Enabled IScsi_SUPPORT on Purley generation.
22.[Enhancements] Modify the allocated buffer from EfiBootServicesData to EfiRuntimeServicesData.
23.[Enhancements] Disable MROM1 device since product doesn't use Intel IE function.
24.[Enhancements] Update DBX file to fix Secure Boot Bypass issue.
25.[Enhancements] Update AMI label 5.14_PurleyCrb_0ACLA057 for RC0623.D09 2022.3 IPU. (1) 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), CVE-2022-29515(6.0 Medium) (2) For INTEL-TA-00688 Security Advisory to address CVE-2022-26006 (8.2 High), CVE-2022-21198(7.9 High)
26.[Enhancements] Update Intel DCPM UEFI driver to 1.0.0.3536.
27.[Fixes] Fix OA2 key injection issue.

3.4(11/03/2020)
1. Changed BIOS revision to 3.4.
2. 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).
3. Updated AMI label 5.14_PurleyCrb_0ACLA052_BETA for RC update and IPU 2020.2 PV to address Intel-TA-00358: CVE-2020-0587 (6.7, Medium), CVE-2020-0591 (6.7, Medium), and CVE-2020-0592 (3, Low); 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); Intel-TA-00391: CVE-2020-8752 (9.4, Critical), CVE-2020-8753 (8.2, Critical), CVE-2020-12297 (8.2, Critical), CVE-2020-8745 (7.3, Critical), CVE-2020-8705 (7.1, Critical), CVE-2020-12303 (7.0, Critical), CVE-2020-8757 (6.3, Medium), CVE-2020-8756 (6.3, Medium), CVE-2020-8760 (6.0, Medium), CVE-2020-8754 (5.3, Medium), CVE-2020-8747 (4.8, Medium), CVE-2020-12356 (4.4, Medium), CVE-2020-8746 (4.3, Medium), and CVE-2020-8749 (4.2, Medium); Intel-SA-00358: CVE-2020-0590 (7.7, High), CVE-2020-0587 (6.7, Medium), CVE-2020-0591 (6.7, Medium), CVE-2020-0593 (4.7, Medium), CVE-2020-0588 (3.8, Low), and CVE-2020-0592 (3.0, Low); Intel-TA-00391: CVE-2020-8744 (7.2, High), CVE-2020-8705 (7.1, High), and CVE-2020-8755 (4.6, Medium); AMI SA50080 and AMI SA50081: CVE-2020-0570 (7.6, High), CVE-2020-0571 (5.5, Medium), and CVE-2020-8675 (7.1, High); AMI SA-50085: CVE-2020-10713 (8.2, High); and AMI SA-50084: CVE-2020-10255 (9, High) security issues.
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 BIOS ACM 1.7.41 and SINIT ACM 1.7.49 PW to address Intel-TA-00358: CVE-2020-0588 (3.8, Low) and CVE-2020-0590 (7.7, High) security issues.
6. Updated SATA/sSATA RAID OPROM/EFI driver to VROC PreOS v6.3.0.1005 PV.
7. Added force next boot to UEFI Shell via IPMI support.
8. Added function to move all LANs to the top of boot priority when IPMI forces PXE.
9. Added inband flash status event log to IPMI MEL.
10. Added support for AOC-AH25G-m2S2TM.
11. Fixed inability of 6240R and some refresh 4 serial CPU frequencies to reach maximum when enabling Mwait.
12. Fixed failure of Secure Erase - Password and problem of BIOS returning "EFI_Device_Error" with SED: Seagate ST1000NX0353.
13. Corrected BMC firmware revision in BIOS Setup.
14. Fixed problem of system hanging at 0xB2 with some NVMe devices.

*3.3 (*05/04/2020)
1. First Release