BIOS Release Notes Form

Product Name	**X12DSC-A6**
Release Version	**2.1**
Release Date	**08/28/2024**
Build Date	**07/11/2024**
Previous Version	**1.4b**
Update Category	**Critical**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1.[Enhancements] Update 5.22_WhitleyCrb_0ACMS_ICX_076_BETA (IPU-PV 2023.3).** **2.[Enhancements] Update BMC/BMC Network Configuration page IPv6 DNS/DNS2 setting.** **3.[Enhancements] Change the strings from "Lock mode" to "Lockdown mode".** **4.[Enhancements] Updated Intel Server Platform Services for Whitley Server Platforms IPU2023.3 4.4.4.500** **5.[Enhancements] Update Dx/Mx BETA microcode for IPU2023.4 Out of band for Intel-SA-00950.** **6.[Enhancements] Update M87606A6_0D0003D1 microcode for Dx/Mx stepping CPU. For INTEL-SA-00950 Security Advisory to address CVE-2023-23583(8.8, High) security issue. For INTEL-SA-00960 Security Advisory to address CVE-2022-41804(6.1, Medium)security issue.**

	7.[Enhancements] Update base to 5.22_WhitleyCrb_0ACMS_ICX_077 (2024.1 IPU-PV) for INTEL-SA-00960 Security Advisory to address CVE-2022-41804(6.1, Medium)security issue. **8.[Enhancements] Updated Intel Server Platform Services for Whitley Server Platforms IPU2024.1 4.4.4.603 for INTEL-SA-00960 Security Advisory to address CVE-2022-41804(6.1, Medium)security issue.** **9.[Enhancements] Update AMITSE module for AMI SA50216 Security Advisory(LogoFAIL Vulnerability) to address CVE-2023-39538(7.5, High) and CVE-2023-39539(7.5, High) security issues.** **10.[Enhancements] Expose item Pre-boot DMA Protection.** **11.[Enhancements] Update kernel to 5.22_WhitleyCrb_0ACMS_ICX_079 (2024.3 IPU).** **12.[Enhancements] Rollback secure boot MS2026 KEK and DB to fix SGX registration failure issue.** **13.[Enhancements] Apply AMI SA50235 for extended parser corruption correction.** **14.[Enhancements] Apply AMI SA50232 to address predictable TCP initial sequence numbers. 1. CVE-2023-45236 Use of a Weak PseudoRandom Number Generator (Risk Level : 5.8). 2. CVE-2023-45237 Predictable TCP initial sequence numbers (ISNs) generated by the TCP/IP stack (Risk Level : 5.3).** **15.[Enhancements] For SA50243 (CVSS3.1 (7.5, High)) fix that UsbRtSmm module has a TOCTOU vulnerability.** **16.[Enhancements] Patch for Mellanox InfiniBand Controller MAC Address issue.** **17.[Enhancements] Update Dx/Mx microcode for IPU2024.3 Security Advisory. For INTEL-SA-01071 Security Advisory to address CVE-2023-43758(8.2, High), CVE-2023-42772(8.2, High), CVE-2024-23599(7.9, High), CVE-2023-41833(7.5, High), CVE-2023-34440(7.5, High), CVE-2024-21829(7.5, High), CVE-2023-43626(7.5, High), CVE-2024-21871(7.5, High), CVE-2024-21781(7.2, High), CVE-2023-23904(6.1,**

	Medium), CVE-2023-22351(6.1, Medium), CVE-2023-43753(5.3, Medium) and CVE-2023-25546(2.5, Low) security issures. For INTEL-SA-01079 Security Advisory to address CVE-2024-21820(7.2, High) and CVE-2024-23918(8.8, High) security issue. For INTEL-SA-01083 Security Advisory to address CVE-2024-24853(7.2, High) security issue. For INTEL-SA-01097 Security Advisory to address CVE-2024-24968(5.3, Medium) security issue. For INTEL-SA-01100 Security Advisory to address CVE-2024-25980(6.1, Medium) security issue. For INTEL-SA-01103 Security Advisory to address CVE-2024-23984(5.3, Medium) security issue. For INTEL-SA-01118 Security Advisory to address CVE-2024-25939(6.0, Medium) security issue.
New features	**N/A**
Fixes	**1.[Fixes] Fix incorrect total memory size on setup if install 6 memory.** **2.[Fixes] Fix memory still is mapped out because of UECC even after AC cycle.** **4.[Fixes] Fixed the issue that SMBIOS Type0 System Family change 3ould not be preserved after clearing CMOS.**

Release Notes from Previous Release(s)

1.4b(04/13/2023)

1.[Enhancements] Update 5.22_WhitleyCrb_0ACMS_ICX_73 Intel BKCWW40 PLR3 OOB, please check header for firmware revisions.
2.[Enhancements] Update M87606A6_0D00037B microcode for Dx/Mx stepping CPU.
3.[Enhancements] Update VROC SATA/sSATA EFI driver to VROC PreOS v7.8.0.1012 to address Intel Virtual RAID on CPU (VROC): Data Loss Exposure Due to RAID 5 TRIM Support document #737276
4.[Enhancements] Update DBX file to fix Secure Boot Bypass issue.
5.[Enhancements] Follow the SMBIOS template sync the chassis type from FRU0 to SMBIOS Type 03.
6.[Enhancements] Update 5.22_WhitleyCrb_0ACMS_ICX_74 Intel BKCWW46 IPU2023.1, please check header for firmware revisions.
7.[Enhancements] Updated Intel Server Platform Services for Whitley Server Platforms IPU2023.1 4.4.4.301

1.4 (07/14/2022)

1.[Enhancements] Update BIOS version to 1.4.
2.[Enhancements] Update AMI 5.22_WhitleyCrb_0ACMS_ICX_070_BETA RC27P52 for BKC 2021_WW52 (PLR1)

3.[Enhancements]Change string "VMX" to "Intel Virtualization Technology"
4.[Fixes] Remove 1G option from MMCFG base to avoid system hang.
5.[Fixes] Fixed the SMBIOS event log ERROR CODE not display correctly under BIOS menu issue (EFI error type).
6.[Fixes] Correct "PCIe ASPM Support (Global)"" default value to disable.
7.[Fixes]Rollback VROC SATA/sSATA EFI driver to VROC PreOS v7.6.0.1012 to fix system hang when VMD enable.

1.0 (11/08/2021)
1. *First Release.*