BIOS Release Notes Form

Product Name	**X12DHM-6**
Release Version	**2.1 SPS: 4.4.4.603**
Build Date	**07/05/2024**
Previous Version	**1.8 SPS: 4.4.4.603**
Update Category	**Recommended**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Updated kernel to 5.22_WhitleyCrb_0ACMS_ICX_079_BETA (2024.3 IPU).** **2. Applied AMI SA50232 to address the security vulnerabilities listed below:** **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).** **3. Applied SA50218 supplement (Vulnerability In EDK2 NetworkPkg).** **4. Applied SA50230 supplement (Image Parser Corruption Vulnerability).** **5. For SA50243 (CVSS3.1 (7.5, High)), fixed the UsbRtSmm module that had a TOCTOU vulnerability.** **6. Disabled PSUs Monitoring function (PSUs).**
New features	**None**

Fixes	**1. Resolved IPMI PXE boot fails after installing OS.**

Release Notes from Previous Release(s)

1.8 SPS: 4.4.4.603 (11/22/2023)

1. *Updated base to 5.22_WhitleyCrb_0ACMS_ICX_077.*
2. *Updated Dx/Mx PC microcode Intel-Restricted-2024-1-IPU-20231009_20241IPU for IPU2024.1.*
3. *Fixed system stuck at 0xB2 when plugging BPS with MM mode.*
4. *Updated Intel Server Platform Services for Whitley Server. Platforms IPU2024.1 4.4.4.603.*

1.6 (6/21/2023)

1. Updated BIOS revision to 1.6.
2. Updated 5.22_WhitleyCrb_0ACMS_ICX_076_BETA (IPU-PV 2023.3).
3. Changed the strings from "Lock mode" to "Lockdown mode".

1.5 SPS: 4.4.4.301 (4/26/2023)

1. *Added ECM RNDIS support.*
2. *Fixed no boot option for single HDD under RAID mode.*
3. *Fine-tuned VROC key detection function.*
4. *Updated BIOS revision to 1.5.*
5. *Updated 5.22_WhitleyCrb_0ACMS_ICX_075 Intel 2023.2 IPU-PV.*

1.4b (1/20/2023)

1. *Updated 5.22_WhitleyCrb_0ACMS_ICX_74 Intel BKCWW46 for IPU2023.1, please check header for firmware revisions.*
2. *Updated 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).*
3. *Followed CPLD spec to set BIOS_EXIT_UBOOT and BIOS_BOOT_OK for VRM I2C Protect.*
4. *Followed the SMBIOS template to sync the chassis type from FRU0 to SMBIOS Type 03.*
5. *Updated Intel Server Platform Services for Whitley Server Platforms.*
6. *Changed BIOS revision to 1.4b.*
7. *Fixed system will not attempt Legacy PXE boot to even set the network to first priority when there is another legacy OS on the system issue.*
8. *Fixed VMWARE passthrough malfunction issue.*
9. *Fixed Linux OS will show an ACPI warning message during the reboot issue.*
10. *Fixed system hang on 0xA9 after setting MMCFG base to 1.5G and 1.75G*
11. *Fixed BIOS send incorrect VMD bitmap setting to SYS-220H-TN24R system with BPN-NVMe4-HS219N-S24 issue.*

1.4 (7/12/2022)

1. *Updated 5.22_WhitleyCrb_0ACMS_ICX_72 Intel BKC WW23 PLR3, please check header for firmware revisions.*
2. *Updated VROC SATA/sSATA EFI driver to VROC PreOS v7.7.6.1004 to adress INTEL-TA-00692.*
3. *Added "CSM Support" setup item into SMCISBForm page.*
4. *Filtered Dynamic TCG Security Pages to patch SUM ChangeBiosCfg failed problem*
5. *Fixed SUM ChangeBiosCfg command cannot update PchSetup variable related BIOS items issue.*
6. *Improved get VPD data routines for E810.*
7. *Now supports IPMI PXE boot to all LAN port feature for both Legacy and UEFI PXE.*
8. *Applied workaround to fix Linux OS show incorrect CPU max frequency issue.*

9. *Updated SmcOOB to the version "_SMCOOBV1.01.25_" to fix the unexpected system-reseting when loading NVRAM defaults.*

1.2 (2/17/2022)

1. *Removed 1G option from MMCFG base, to avoid system hang.*
2. *Fixed the SMBIOS event log ERROR CODE which is not displaying correctly under BIOS menu issue (EFI error type).*
3. *Fixed SpeedStep (P-States) setting change, when its default setting is set to Disable, and loaded BIOS defaults in Setup.*
4. *Fixed COM port resource where it can't be changed, and the item's intended function does not work.*
5. *Updated AMI 5.22_WhitleyCrb_0ACMS_ICX_070 RC27P56 for BKC 2021_WW52 (PLR1 HF)2.*
6. *Changed string "VMX" to "Intel Virtualization Technology".*
7. *Added flag [Preserve BIOS Boot Options Configuration] controlled by BMC/SUM.*
8. *Changed BIOS revision to 1.2.*
9. *Updated PLR1 HF RC27P56, microcode M87606A6_0D000332d*

1.1a (10/12/2021)

Enhancements
1. Updated 5.22_WhitleyCrb_0ACMS_ICX_067 Intel BKCWW32 2021 PV MR5.
2. Updated Dx/Mx microcode from Intel-Generic-Microcode-20210804_NDA.
3. Updated SPS 4.4.4.58 PV MR5.
4. Changed BIOS revision to 1.1a.
5. Changed "Hard Drive Security Frozen" default setting to disabled.
6. Disabled support for EFI iSCSI.
7. Added support for SUM upload/delete HTTPS TLS certificate.
8. Updated BIOS/SINIT ACM 1.0.D.
9. Set CPU1 AIOM x16 slot OPROM control item and IIO port item to show whether AIOM1 slot has device or not.
10. Modified NVMe slot IIO port string.
Fixes
1. Fixed inability to detect BPN-SAS3-LA26A-N12 v2.00.
2. Fixed malfunction of OnBoardLanCheck workaround.
3. Fixed inability to change COM port resource and failure of item's behavior.
4. Added support for i350 UEFI PXE boot of AIOM2 slot for SYS-220HE-FTNR and SYS-620H-TN12R systems.
5. Corrected NVMe OPROM control item shown in BIOS menu with 9/16 1.1A ECO BIOS.
6. Fixed issue with POST looping at 94h with AIOM2 populated on AOM-AIOM-2X8.

1.1 (4/30/2021)

1. Updated RC 20.P96 for PV RC update.
2. Changed BIOS revision to 1.1.