BIOS Release Notes

Product Name	**X12DDW-A6**
Release Version	**2.1 SPS: 4.4.4.603**
Build Date	**07/04/2024**
Previous Version	**1.9 SPS: 4.4.4.603**
Update Category	**Recommended**
Dependencies	**None**
New features	**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 eak 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 where the UsbRtSmm module had a TOCTOU vulnerability.**

Fixes	1. **Resolved how IPMI PXE boot failed after installing OS.** 2. **Resolved how the boot order could not be adjusted by AMI SCE.**

1.9 SPS: 4.4.4.603 (01/11/2024)

1. *Updated the 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.*
2. *Exposed "Pre-boot DMA Protection".*
3. *Updated source base to 5.22_WhitleyCrb_0ACMS_ICX_077 (2024.1 IPU-PV).*
4. *Updated Dx/Mx PC microcode Intel-Restricted-2024-1-IPU-20231009_20241IPU for IPU2024.1.*
5. *Updated Intel Server Platform Services for Whitley Server Platforms IPU2024.1 4.4.4.603.*
6. *Fixed how ATT Test case "Check BBS test" failed when using Windows OS for test problem.*
7. *Fixed system stuck at 0xB2 when plugging BPS with MM mode.*
8. *Fixed how HostInterface On/Off test will drop in four times in UEFI Shell.*
9. *Resolved how KMS configuration could not be preserved after load BIOS default.*
10. *Fixed how HostInterface On/Off test will drop in four times in UEFI Shell. (Refer to EagleStream SVN3178.)*
11. *Displayed dynamic gateway IPV6 address as ":::::::" on BIOS setup if dynamic router info set count is 0.*
12. *Displayed static gateway IPV6 address as ":::::::" on BIOS setup if it could not get valid gateway IPV6 address through IPMI.*

1.7 (09/26/2023)

1. *Support Whitley Server Platforms.*
2. *Updated BMC/BMC Network Configuration page IPv6*
3. *DNS/DNS2 setting.*
4. *Updated the USB keyboard code to fix scanner input issue.*
5. *Updated x-AMI ID for PCH VMD mode.*
6. *Updated Dx/Mx microcode with IPU2023.4 out of band for*
7. *Intel-TA-00950.*
8. *Fixed ENERGY_PERF_BIAS_CFG Mode item change to default after SUM update BIOS with --preserve_setting command.*
9. *UECC mapped out DIMM information can only be removed by clearing CMOS.*
10. *SMBIOS Type0 System Family change not preserved after clearing CMOS.*
11. *System stops POSTing at A9 when installing large MMIO request AOC on system such as AOC-A25G-i4SM.*
12. *DIMM total memory size shown incorrectly in setup.*
13. *Resolved IPV6 "Gateway IP" is not displayed correctly.*

1.5 (05/04/2023)

1. Updated 5.22_WhitleyCrb_0ACMS_ICX_075 Intel 2023.2 IPU-PV, please check header for firmware revisions.
2. Pulled high GPP_C10_FM_PCH_SATA_RAID_KEY first before VROC key detection.
3. Modified GetVariable() service for buffer overflow in certain cases.
4. Fixed system hang on 0xA9 after setting MMCFG base to 1.5G and 1.75G.
5. Fixed the SUM TC: 2020 test fail problem.
6. Added a workaround for VRM.

1.4b (01/12/2023)

1. Updated 5.22_WhitleyCrb_0ACMS_ICX_74 Intel BKCWW46. Please check the header for firmware revisions.
2. Enhancements when running the SUM TC: 220/271/356/457/2071/3056/4057 with Windows OS caused the boot order compare fail after flash BIOS.
3. Removed mapping ID of IIO port 42.
4. Fixed an issue where memory errors were not being reported in the SMBIOS event log.

1.4a (11/24/2022)

1. Updated 5.22_WhitleyCrb_0ACMS_ICX_73 Intel BKCWW40 PLR3 OOB. Please check the 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 sync the chassis type from FRU0 to SMBIOS Type 03.
5. Updated Intel Server Platform Services for Whitley Server Platforms IPU2023.1 4.4.4.301.
6. Fixed the system will not attempt Legacy PXE boot even set network to first priority when there is other legacy OS on the system issue.

1.4 (08/04/2022)

1. Updated 5.22_WhitleyCrb_0ACMS_ICX_72 Intel BKC WW23 PLR3. Please check the header for firmware revisions.
2. Updated VROC SATA/sSATA EFI driver to VROC PreOS v7.7.6.1004 to address 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. Enhanced get VPD data routines for E810.
6. Supported IPMI PXE boot to all LAN port feature for both Legacy and UEFI PXE.
7. Apply workaround to fix Linux OS showing the incorrect CPU max freq issue.
8. Updated SmcOOB to the version "_SMCOOBV1.01.25_" to fix the unexpected system-resetting when loading NVRAM defaults.
9. Exposed Link Retrain per port, exposed MCTP for CPU1 slot1 and CPU2 slot2 in BIOS.
10. If chassis type of FRU0 is not 1(other) or 2(unknown), synced it to SMBIOS type 3.
11. Fixed the SUM ChangeBiosCfg command could not update PchSetup variable related BIOS items issue.

12. *Updated VPD routine.*

1.2 (02/14/2022)

1. *Updated AMI 5.22_WhitleyCrb_0ACMS_ICX_070 RC27P52 for BKC 2021_WW52 (PLR1)*
2. *Changed string "VMX" to "Intel Virtualization Technology".*
3. *Added 12+2 NVMe config support.*
4. *Removed 1G option from MMCFG base to avoid system hang.*
5. *Removed unused ACPI device to fix FWTS fail item.*
6. *Fixed how the SMBIOS event log ERROR CODE was not displaying correctly under BIOS menu issue (EFI error type).*
7. *Added "Preserve_SMBIOS", "Preserve_OA" into FlashFlag when in the condition "NvramDefaultMode".*
8. *Fixed the setup item "Lockdown Mode" always gray-out.*

1.1b (09/18/2021)

1. *Enable 2U non-NVMe system support with 668 RSC.*

1.1 (05/10/2021)

1. *Set default Boot Guard profile to 5.*
2. *Set all oprom control items to Legacy when boot mode was set to Dual.*
3. *Updated CPLD Signature table 101 and tool to 1.30.24 for CPLD Signature table 101.*
4. *Supported 6+4 NVMe solution.*
5. *Added new CPU power spec profiles.*
6. *Fixed how T-states always showed 15 levels even when T-state was disabled.*
7. *Offboarded no output in Setup if we limit to 4G in Non-EFI mode.*
8. *Fixed the issue that Microsoft HLK certification, TPM 2.0 UEFI Preboot Interface Test, failed on Microsoft Server 2019.*
9. *Fixed a CPU exception problem.*
10. *Fixed how the SmcSecureErase setup page wasn't hidden when not HDD devices were plugged in.*
11. *Fixed how the UEFI OS boot option name showed incorrectly in BIOS setup.*
12. *Fixed Secure Boot Append/Update Keys failed problem.*
13. *Fixed the issue that all OOB files could not be uploaded if BMC is first boot.*
14. *SMBIOS type 16 Number of Memory Devices.*
15. *Followed template to correct iSCSI Configuration page.*
16. *Recalibrated DIMM size when rank is disabled.*
17. *Fixed the issue that system hangs up after executing sum -c EraseOAKey or afuefi /OAD.*

1.0b (03/03/2021)

1. *Updated BKCWW09 2021 (PCIe recipe 3.8). Please check header for firmware revisions.*
2. *Updated Intel-Generic-Microcode-20210226a_NDA and Intel AE.*
3. *Updated ASPEED VBIOS and EFI driver to 1.11.03.*
4. *Updated SATA/sSATA EFI driver to VROC PreOS v7.5.0.1152.*
5. *Kept value of setup string of Manufacturer and Product according to priority "modification of AmiBcp, FUR1 and then SMBIOS Table".*

6. *Added code to stop AFU support.*
7. *Added HCC Mx stepping CPU check for CPU stepping display.*
8. *Automatically disabled and hid ADDDC with x8 width DIMM.*
9. *Auto hid "NVMe Firmware Source" when AOC-SMG3-2M2-B was plugged.*
10. *Disabled MCTP for M.2 slots to avoid system hang with Micron 2300.*
11. *Removed intel lan memory 4G limit if boot mode is not legacy.*
12. *Automatically disabled and grayed out ADDDC, UMA-Base Clustering, mirror mode, and enable NUMA when SGX enabled.*
13. *Enhanced SMCI HDD Security feature.*
14. *Extended memory DIMM serial number information. (Samsung, Micron, Hynix)*
15. *Enhanced Smc Dcpmm feature.*
16. *Added RSC-D2-666-G4 and RSC-D2R-666-G4.*
17. *Fixed how SUT won't prompt "Enter User password" screen after setting a password when plugging in SED device.*
18. *Fixed the IPv4 IPv4 address source status showing incorrect after updating BIOS issue.*
19. *SMBIOS type 17 was missing BPS information when plugged at P1-DIMMC2 or P2-DIMMC2.*
20. *Fixed wrong location of RT UECC log.*
21. *Fixed RT UECC was not mapped out.*
22. *Fixed IPV6 disable in the IPMI GUI but BIOS initialize will appear IPV6 address.*
23. *Filtered Dynamic HDD Security Pages to patch SUM ChangeBiosCfg failed problem.*
24. *Fixed GPU sensor issue with 2U riser.*

1.0a (01/04/2021)

1. *Updated BKC to WW51 PC2.*
2. *Added retrain for X550 AIOM link drop.*
3. *Added F1 reboot function upon password 3 times try out.*
4. *Turned on MCTP for BMC usage.*
5. *Added NVMe VMD auto mode: enable VMD when VROC key present and disable VMD when VROC key absent.*

1.0 (10/27/2020)

1. *First release based on BKC WW41.*

_____   _____

Product Manager   *Date*