BIOS Release Notes Form

Product Name	**X12STW-(T)F**
Release Version	**1.4**
Build Date	**12/22/2022**
Previous Version	**1.2**
Update Category	**Recommended**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Updated the Microcode A0671 to 0x57 and A0653 to 0xF4 per IPU 2023.1 Processor Advisory INTEL-TA-00767 to address CVE-2022-38090 (6.0 Medium). Updated the security for AMISV304 (SA50121).** **2. Updated the ACM version to 1.14.46 (20220819) per IPU 2023.1 Processor Advisory INTEL-TA-00767 to address CVE-2022-30704 (7.2 High).** **3. Updated the SPS ME firmware to SPS_E3_06.00.03.309.0 per IPU 2023.1 Processor Advisory INTEL-TA-00718 to address CVE-2022-36794 (6.0 Medium).** **4. Updated EfiOsBootOptionNames and relevant dependencies for Security update.**

	5. Modified the options of "Gen3 ASPM Control" and "Gen3 ASPM" to match loading defaults by pressing F3.
New features	**N/A**
Fixes	**N/A**

Release Notes from Previous Release(s)

1.2 (8/2/2022)

1. Updated the BIOS version to 1.2.
2. Synced chassis type of SMBIOS type 3 from FRU0 and override it if modified by the AMIDMIEDIT tool.
3. Applied a patch according to the AMI Customer Advisory document UefiNetworkStack Aptio 5.x SA50110.
4. Updated the RC chipset based on AMI Tatlow Server source code label 16 (BETA) 5.22_1AXCT_RC0B.01.34.60_016.
5. Updated the "Security Erase Configuration" string to "SMCI Security Erase Configuration."
6. Filtered the Dynamic TCG Security Pages to patch SUM ChangeBiosCfg failed problem.
7. Updated Microcode to 0x54 for IPU 2022.1 SGX Advisory INTEL-TA-00614 to address CVE-2022-0005 (4.9 Medium), Processor Advisory INTEL-TA-00617 to address CVE-2022-21151 (5.3 Medium) and Security Advisory INTEL-TA-00615 to address CVE-2022-21166 (5.5 Medium)
8. Updated BIOS ACM and SINIT ACM to 1.14.39 (20211214) for 2022.1 IPU – BIOS Advisory, INTEL-TA-00601 to address CVE-2021-33123 (8.2 High), CVE-2021-33124 (7.5 High) and CVE-2021-33103 (7.5 High)
9. Enhanced IPv6 feature according to "Proposal for BIOS-BMC IPv6 inconsistency ver. 14.".
10. Updated Microcode to 0x54 per IPU 2022.2 Processor Advisory INTEL-TA-00657 to address CVE-2022-21233 (6.0 Medium).
11. If the FRU0 chassis type is not 1 or 2, synchronize the FRU0 chassis type to SMBIOS type 3.
12. No boot option for single HDD under RAID mode.
13. Updated AHCI driver from ver 23 to ver 28
14. Enhanced the setup options Enable Root Port, Max Link Speed, and ASPM of PEG Port Configuration.
15. Enhanced the storage monitoring information not showing in the webGUI after AOC-3908L-H8IR is switched to PCIe mode.
16. Added the current boot device name in the SUM OOB dump .
17. Followed the SMBIOS template to synchronize the chassis type from FRU0 to SMBIOS Type 03.
18. Fixed a hang at post code 2F when updating BIOS from 1.1 to 1.2 via BMC web or SUM.

19. Fixed I210 Legacy PXE boot.

1.2 (7/6/2022)

1. Updated the BIOS version to 1.2
2. Synced chassis type of SMBIOS type 3 from FRU0. override it if modified by tool(AMIDMIEDIT)
3. Applied patch per AMI Customer Advisory document UefiNetworkStack Aptio 5.x SA50110
4. Based on AMI Tatlow Server source code label 16 (BETA) 5.22_1AXCT_RC0B.01.34.60_016 to update RC chipset.
5. Updated "Security Erase Configuration" string to "SMCI Security Erase Configuration".
6. Filtered Dynamic TCG Security Pages to patch SUM ChangeBiosCfg failed problem Update 7. Microcode to 0x54 for IPU 2022.1 SGX Advisory INTEL-TA-00614 to address CVE-2022-0005 (4.9 Medium), Processor Advisory INTEL-TA-00617 to address CVE-2022-21151 (5.3 Medium) and Security Advisory INTEL-TA-00615 to address CVE-2022-21166 (5.5 Medium)
7. Updated BIOS ACM and SINIT ACM to 1.14.39 (20211214) for 2022.1 IPU – BIOS Advisory, INTEL-TA-00601 to address CVE-2021-33123 (8.2 High), CVE-2021-33124 (7.5 High) and CVE-2021-33103 (7.5 High)
8. According to "Proposal for BIOS-BMC IPv6 inconsistency ver. 14", enhancement for the IPv6 feature.
9. Updated Microcode to 0x54 per IPU 2022.2 Processor Advisory INTEL-TA-00657 to address CVE-2022-21233 (6.0 Medium)
10. If chassis type of FRU0 is not 1(other) or 2(unknown), sync it to SMBIOS type 3.
11. No boot option for single HDD under RAID mode.
12. Updated AHCI driver from ver 23 to ver 28
13. Setup options e.g. Enable Root Port, Max Link Speed , ASPM of PEG Port Configuration malfunction.
14. The Storage Monitoring does not show in WEBUI after AOC-3908L-H8IR switch to PCIE mode.
15. Added fill in the current boot device name in the SUM OOB dump information.
Fixed the following issues:
16. An unknown device with _HID INTC1025(yellow bang) found when Intel® Trusted Execution Technology (Intel® TXT) is enabled under Windows Server 2022 and 2019. no functional impact and everything works as expected*
17. Hang at post code 2F if updating BIOS from 1.1 to 1.2 via BMC web or SUM.

1.1 (1/21/2022)

1. Updated the BIOS version to 1.0a
2. Hid "Internal Graphics" setup option if there is no graphics engine within this CPU.
3. Based on AMI Tatlow Server source code label 15 (5.22_1AXCT_RC0B.01.34.60_015), updated RC chipset.
4. Updated BIOS ACM and SINIT ACM
5. Fixed Intel PEG port width drop and PEG port speed drop.
6. Update the SPS ME firmware to SPS_E3_06.00.03.039.
Fixed the following issues:
1.KMS operation hang (Create-Key, Get-Key).
2. Onboard EFI LAN OPROM does not load when Boot mode is set to DUAL and LAN OPROM is set to EFI.
3. The memory module in DIMMB2, when the ECC/UECC is active, a GPNV error log will report as DIMMA2.
4. When the ECC/UECC is triggered, it reports an empty memory slot.

5. REFRESH_2X_MODE option is missing, the defaulut setting for GNA Device (B0:D8:F0) and DMA Control Guarantee is changed.
6. Updated SmcOOB SMCOOBV2.00.11 to fix the SUM TC: 239/326/426 sometimes will be fail problem.
7. BMC can't use standard Redfish API to create BootOption.
8. "Lockdown Mode" loses the "<LicenseRequirement>SFT-DCMS-SINGLE</LicenseRequirement>" string in the XML file of SUM.
9. Manufacturer is unknown in BIOS setup when using InnoDisk DIMMs.
10.System hangs while disabling Monitor MWait in BIOS setup.

1.0a (11/05/2021)

1. *Fixed an issue that when disabling BMC IPv6 Support in the BIOS, the IPv6 Address Status will show "Disabled" instead of "_".*
2. *Fixed issue where when the PCIe PERR is triggered, no events are recorded in the Event Log.*
3. *Fixed system Recovery hang on 0x94 after BIOS crash under Dual mode.*
4. *Fixed an issue that when testing the USB port mapping, it returns an incorrect port under WHQL.*
5. *Fixed serial number in SMBIOS type 17, as it loses bytes when using Samsung DDR4 memory.*
6. *Fixed SMCIPMITOOL/IPMICFG where it can't set persistent boot under DUAL mode, and Legacy mode through IPMI Boot Flag Command.*
7. *Fixed susceptibility to DDR4 Rowhammer attacks.*
8. *Enabled the SR-IOV item in the PCI page.*
9. *Added Intel PEG port width drop workaround and PEG port speed drop workaround.*
10. *Added Intel IPS #00641060 patch to support disabling of AVX/AVX3. Added AVX and AVX3 setup items.*
11. *Updated Microcode to M02A0671_0000004C.*
12. *Added a switch on the SMBUS to channel 0 to avoid an SMBUS address conflict.*
13. *Modified the i210 UEFI/Legacy option ROM version in the OFID table.*