BIOS Release Notes Form

Product Name	**X12STH-F/LN4F/SYS**
Release Version	**1.8**
Build Date	**1/3/2024**
Previous Version	**1.6**
Update Category	**Recommended**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Updated BIOS version to 1.8.** **2. Updated AMI SA50216 Supplement for Security Advisory to address CVE-2023-39539 (7.5, High) security issue.** **3. SA50218 Supplement for update to fix seven exploitable security issues in the TianoCore EDK2 NetworkPkg integrated into AptioV. CVE-2023-45229 (6.5, Medium), CVE-2023-45230 (8.3, High), CVE-2023-45231 (6.5, Medium), CVE-2023-45232 (6.5, Medium), CVE-2023-45233 (6.5, Medium), CVE-2023-45234 (8.3, High), and CVE-2023-45235 (8.3, High).** **4. SA50230 Supplement to address CVE-2023-39539 (7.5, High) security issue.** **5. Updated Microcode A0671 to 0x5E and A0653 to 0xFA per IPU 2024.1.**

	6. Updated SPS FW to 6.0.3.604 per IPU 2024.1. **7. Updated RC for IPU 2024.1 RC2124_50 PV.** **8. Grayed out "Preferred DNS server IP" and "Alternative DNS server IP".** **9. Added Rocky Linux into the BIOS default identical OS list.**
New features	**N/A**
Fixes	**1. Fixed how a total HD capacity of more than 26T will cause incorrect BIOS menu HD information PBID:168341.**

Release Notes from Previous Release(s)

1.6 (6/7/2023)

1. *Update BIOS version to 1.6.*
2. *Updated Microcode A0653 to 0xf8 and A0671 to 0x59 per IPU 2023.3 Processor Advisory INTEL-TA-00828 to address CVE-2022-40982 (6.5 Medium).*
3. *Updated RC per IPU 2023.3 Processor Advisory.*
4. *Updated the SPS ME firmware to SPS_E3_06.00.03.505.0 per IPU 2023.3 Processor Advisory.*
5. *Updated the BMC/BMC Network Configuration page IPv6 DNS/DNS2 setting.*
6. *Added insert Secure boot key via SUM/Redfish.*
7. *Updated missing files of f3bb79b1ffb6a98bef254a236cace547f86f171c.*

1.4a (02/22/2023)

1. *Updated BIOS version to 1.4a.*
2. *Fixed the issue where the BIOS did not provide the "Onboard LAN1 Support" and "Onboard LAN2 Support" in Redfish JSON.*

***1.4 (12*/22/2022)**

1. *Updated the BIOS version to 1.4.*
2. *Updated 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 security for AMISV304 (SA50121).*
3. *Updated ACM version to 1.14.46 (20220819) per IPU 2023.1 Processor Advisory INTEL-TA-00767 to address CVE-2022-30704 (7.2 High).*
4. *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).*
5. *Updated EfiOsBootOptionNames and relevant dependencies for Security update.*
6. *Modified the options of "Gen3 ASPM Control" and "Gen3 ASPM" to match loading defaults by pressing F3.*

***1.2 (*05/19/2022)**

7. *Updated the BIOS version to 1.2.*
8. *Updated Microcode to 0x54 per IPU 2022.2 Processor Advisory INTEL-TA-00657 to address CVE-2022-21233 (6.0 Medium).*
9. *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).*
10. *Based on AMI Tatlow Server source code label 16 (BETA) 5.22_1AXCT_RC0B.01.34.60_016, updated RC chipset.*
11. *Sync chassis type of SMBIOS type 3 from FRU0, override it if modified by tool(AMIDMIEDIT).*
12. *Updated AHCI driver from ver 23 to ver 28.*
13. *Added boot option for single HDD under RAID mode.*
14. *If chassis type of FRU0 is not 1(other) or 2(unknown), sync it to SMBIOS type 3.*
15. *After loading BIOS default in BIOS setup, ISH (B0:D12h:F0) will be disabled.*
16. *System cannot power on if proceed BIOS recovery from 1.0a to 1.1 or from 1.1 to 1.0a.*
17. *System with PCIe card stuck in reset loop while running TC:Check the Behavior of BIOS FDT Changed.*
18. *Added the plain-text password support to SMC-OOB2.*
19. *Fixed hang at post code 2F if updating BIOS from 1.0a to 1.1 via BMC web or SUM.*
20. *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.*
21. *Fixed setting "BootSourceOverrideEnabled" via Redfish issue.*
22. *Boot options will miss when use SUM to clear httpboot.*

1.0a (12/13/2021)

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 the WHQL test USB port that is mapping incorrectly.*
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. *Corrected issue where the BIOS password is lost after update.*
8. *Fixed SUM testing issue where the password is not retained.*
9. *Corrected issue when using the AFU flash tool to update the BIOS, the BIOS Build Date will not change in the BIOS setup menu.*
10. *Fixed issue where system is unable to sync on SMbios type2 when changing product name of fru1 by the IPMICFG utility.*
11. *Updated support for SUM V2.00.11 to fix intermittent failures related to password.*
12. *Added Intel PEG port width drop workaround and PEG port speed drop workaround.*
13. *Added Intel IPS #00641060 patch to support disabling of AVX/AVX3. Added AVX and AVX3 setup items.*
14. *Based on Tatlow_Server_BKC_2021_WW39_PLR1, updated BtG BIOS ACM version to 1.14.26 (20210902) and SINIT ACM version to 1.14.26 (20210902).*

15. *Based on AMI Tatlow Server source code label 14 (5.22_1AXCT_RC0B.01.34.60_014) , updated RC chipset.*