

BIOS Release Notes Form

Supermicro disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade. All products, computer systems, dates, and figures specified are preliminary based on current expectations, and are subject to change without notice. Supermicro and the Supermicro logo are trademarks of Super Micro Computer, Inc. in the U.S. and/or other countries. Copyright © 2018 Super Micro Computer, Inc. All rights reserved.

Product Name	X12STH-F/LN4F/SYS
Release Version	1.4
Build Date	12/22/2022
Previous Version	1.2
Update Category	Recommended
Dependencies	None
Important Notes	None
Enhancements	<ol style="list-style-type: none">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.
New features	N/A

Fixes	N/A
--------------	------------

Release Notes from Previous Release(s)

1.2 (05/19/2022)

1. Updated the BIOS version to 1.2.
2. Updated Microcode to 0x54 per IPU 2022.2 Processor Advisory INTEL-TA-00657 to address CVE-2022-21233 (6.0 Medium).
3. 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).
4. Based on AMI Tatlow Server source code label 16 (BETA) 5.22_1AXCT_RCOB.01.34.60_016, updated RC chipset.
5. Sync chassis type of SMBIOS type 3 from FRU0, override it if modified by tool(AMIDMEDIT).
6. Updated AHCI driver from ver 23 to ver 28.
7. Added boot option for single HDD under RAID mode.
8. If chassis type of FRU0 is not 1(other) or 2(unknown), sync it to SMBIOS type 3.
9. After loading BIOS default in BIOS setup, ISH (B0:D12h:F0) will be disabled.
10. System cannot power on if proceed BIOS recovery from 1.0a to 1.1 or from 1.1 to 1.0a.
11. System with PCIe card stuck in reset loop while running TC:Check the Behavior of BIOS FDT Changed.
12. Added the plain-text password support to SMC-OOB2.
13. Fixed hang at post code 2F if updating BIOS from 1.0a to 1.1 via BMC web or SUM.
14. 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.
15. Fixed setting "BootSourceOverrideEnabled" via Redfish issue.
16. 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.*