# 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** | **X12STL-F** |
| **Release Version** | **1.2** |
| **Release Date** | **05/30/2022** |
| **Build Date** | **05/30/2022** |
| **Previous Version** | **1.0a** |
| **Update Category** | **Recommended** |
| **Dependencies** | **None** |
| **Important Notes** | **None** |
| **Enhancements** | **1. Applied patch based on AMI Customer Advisory document UefiNetworkStack Aptio 5.x SA50110.**<br>**2. Changed the text string “Security Erase Configuration” to “SMCI Security Erase Configuration.”**<br>**3. Updated Microcode to 0x53 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).**<br>**4. 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).** |

| | |
|---|---|
| | **5. Changed the chassis type of the FRU0 to SMBIOS type 3 if it is not 1 or 2.**<br>**6. Updated AHCI driver from version 23 to version 28.**<br>**7. Enabled boot option for single HDD under RAID mode.**<br>**8. Updated Microcode to 0x54 per IPU 2022.2 Processor Advisory INTEL-TA-00657 to address CVE-2022-21233 (6.0 Medium).**<br>**9. Filtered Dynamic TCG Security Pages to patch SUM ChangeBiosCfg failed problem.** |
| **New features** | **None** |
| **Fixes** | **1. Fixed an error when an unknown device is installed and Intel® TXT is enabled.**<br>**2. Setup options to Enable Root Port, Max Link Speed , ASPM of PEG Port Configuration malfunction.** |

***Release Notes from Previous Release(s)***

***1.0a (11/18/2022)***

1. *Added Intel PEG port width drop workaround and PEG port speed drop workaround.*
2. *Added Intel IPS #00641060 patch to support disabling of AVX/AVX3. Added AVX and AVX3 setup items.*
3. *Updated Microcode M02A0671_0000004C.*
4. *Added LAN1 and LAN2 Support items in PCIe/PCI/PnP Configuration.*
5. *Fixed an issue that when disabling BMC IPv6 Support in the BIOS, the IPv6 Address Status will show “Disabled” instead of "_".*
6. *Fixed system Recovery hang on 0x94 after BIOS crash under Dual mode.*
7. *Fixed serial number in SMBIOS type 17, as it loses bytes when using Samsung DDR4 memory.*
8. *Fixed SMCIPMITOOL/IPMICFG where it can't set persistent boot under DUAL mode, and Legacy mode through IPMI Boot Flag Command.*
9. *Fixed susceptibility to DDR4 Rowhammer attacks.*