BIOS Release Notes Form

Product Name	**H12SST-PS**
Release Version	**2.3a**
Release Date	**1/25/2022**
Build Date	**1/25/2022**
Previous Version	**2.1**
Update Category	**Recommended**
Dependencies	**N/A**
Important Notes	**BIOS Image:** **BIOS_H12SST-1B45_20220125_2.3a_STDsp.bin** **BIOS Update Package:** **BIOS_H12SST-1B45_20220125_2.3a.zip** **A. Package for upgrade BIOS from version 2.x to version 2.x** **BIOS_H12SST-1B45_20220125_2.3a_STDsp.zip** **B. Package for upgrade BIOS from version 1.x to version 2.0 or above** **BIOS_H12SST-1B45_20220125_2.3a_STDsp_Up.zip** **Important Note:** **1) BIOS R 2.x supports 7002 and 7003 processor.** **2) The Flash Utility in the package supports a BIOS update from R1.x to R 2.x only, this cannot be rolled back.** **3) BIOS R 2.x requires the latest motherboard CPLD before updating. If you purchased the system before 3/13/2021, please contact Supermicro Technical Support to verify before updating the BIOS.** **4) R2.x BIOS default boot mode has been changed to EFI. If your OS is legacy, please press the delete key during POST to enter into the BIOS setting page to change boot mode after upgrading to R2.x.**
Enhancements	**1. Changed BIOS revision to 2.3a.** **2. Added Redfish/SUM Secure Boot feature, update OOB for secure boot and reserve Key.** **3. Added support for SUM upload/delete HTTPS TLS certificate. (Default Enabled by TOKEN "Sum_UploadTlsKey_SUPPORT")** **4. Set Relaxed Ordering default to Enabled.** **5. Updated AGESA RomePI to 1.0.0.C.** **6. Added setup item, "Enhanced Preferred IO Mode".** **7. Updated AGESA MilanPI to 1.0.0.6.** **8. Updated A010 GN B0 microcode 0A001046.**

	Updated A011 GN B1 microcode 0A001137. **Updated A012 GN B2 microcode 0A00121D.** **9. Patched the BMC Redfish Host Interface. It was named ethX when CDN was disabled under Linux OS.** **10. Disabled EFI iSCSI support.** **11. Added setup items "BankGroupSwapAlt", "SEV-SNP Support", "Enhanced Preferred IO Mode" and "Root Complex 0x00~0xE0 LCLK Frequency".**
New features	**N/A**
Fixes	**1. Fixed an issue where SUM cannot modify AMD CBS settings.** **2. Fixed an issue where the SEV feature can't enable on ROT enabled MB.** **3. Fixed an issue that hangs system with a TPM issue.**

Release Notes from Previous Release(s)

2.1 (5/7/2021)

1. Changed BIOS revision to 2.1.
2. Updated AGESA RomePI to 1.0.0.B.
3. Set all OPROM control items to Legacy when boot mode is set to Dual.
4. Removed legacy iSCI support of H12 BIOS.
5. Added force next boot to UEFI Shell support.
6. Updated AGESA MilanPI to 1.0.0.2.
7. Updated A011 GN B1 microcode 0A00111D.
8. Updated USB OC pin mapping to follow motherboard design.
9. Fixed problem of AFU being used to clear event log and then AC cycling the system after BIOS recovery.

2.0 (2/22/2021)

1. Changed BIOS revision to 2.0.
2. Updated AGESA MilanPI to 1.0.0.1.
3. Updated A011 GN B1 microcode 0A001119.
4. Updated AGESA RomePI to 1.0.0.A.
5. Updated 8310 SSP-B0 microcode 830104D.
6. Fixed failures of Fru0 - Manufacturer Name(PM) to sync to SMBIOS Type 3 - Manufacturer(CM) and Fru0 - Product Part/Model Number(PPM) to sync to SMBIOS Type 1 - ProductName(PN).
7. Fixed problem of system hanging on POSTCODE 0xB2 when JPG1 is set to disabled and the VGA card is plugged in.
8. Added SMCI HDD Security feature.
9. Updated help string of item "Input the description".
10. Fixed problem of BIOS initialization showing IPV6 address when IPV6 is disabled in the IPMI GUI.
11. Enhanced SMBIOS Type39 System Power Supply information.
12. Displayed TSME, DDR Power Down Enable, PCIe Ten Bit Support, xGMI Link Width Control, xGMI Force Link Width, xGMI Max Link Width Control, xGMI Max Link Width, and xGMI Link Max Speed for GPU performance tuning.
13. Removed "$SMCUNHIDE$" string from "PCI AER support" setup item help string.
14. Added AMD IOMMU patch code to fix problem of NVMe devices dropping and hardware error occurring in RH 7.x.
15. Fixed bug with TCG admin password reversal.
16. Corrected CPU speed information in BIOS setup**.**

1.1 (2/21/2020)

1. Changed BIOS revision to 1.1.
2. Updated AGESA RomePI to 1.0.0.5 based on 5.14_RomeCrb_0ACMK013.
3. Displayed "PCI AER Support" setup item on ACPI page.
4. Added SMC HDD Security feature.
5. Fine-tuned I2C5 HOLD Setting to 0x00000060, implemented use of token I2C_SDA_HOLD_Fine_Tune_SUPPORT to control it, and set token I2C5_SDA_HOLD_Fine_Tune_SUPPORT to disabled by default.
6. Fixed issue of system hanging at post code A7h.
7. Fixed inability of SUM to change the function of NUMA Node Per Socket.
8. Fixed problem of system sometimes rebooting during legacy Windows 2019 OS installation when using Rome CPU 7502.
9. Removed requirement to use Admin password for erasing TCG device.

1.0c (11/25/2019)

1. Updated BIOS version to 1.0c.
2. Added "DRAM Scrub Time" to Memory Configuration.
3. Updated AGESA RomePI to 1.0.0.4 based on 5.14_RomeCrb_0ACMK012.
4. Set AMD CBS "PCIe ARI Support" item to be used instead of "ARI Forwarding".
5. Updated item string "Input the description" and "HTTP Boot One Time" to adhere to Rome BIOS Setup Template v0.7_20190705.
6. Displayed 3rd IPMI version in BIOS setup.
7. Updated SSID of AMD Host Bridge according to each project's board ID.
8. Set IOMMU default to Auto (Enabled)
9. Displayed "Preferred IO" item.
10. Prevented display of any AMD memory error messages during the POST phase.
11. Fixed malfunction of recovery.
12. Added support for OOB SATA HDD information and asset information of 2 SATA controllers.
13. Fixed missing screen output when Boot Mode is changed to EFI.
14. Fixed the issue of "SMCI POST Screen Message" appearing on BIOS setup menu.
15. Fixed the issue of "SMCI POST Screen Message" appearing on POST screen when executing EFI Shell application.
16. Fixed problem of SR-IOV enable Onboard LAN Option ROM item hiding.

1.0 (8/16/2019)

Initial Release