BIOS Release Notes Form

Product Name	**H12SST-PS**
Release Version	**3.1**
Release Date	**01/20/2025**
Build Date	**01/20/2025**
Previous Version	**3.0**
Update Category	**Recommended**
Dependencies	**N/A**
Important Notes	**BIOS Image:** **BIOS_H12SST-1B45_20250120_3.1_STDsp.bin** **BIOS Update Package:** **A. Package for upgrade BIOS from version 2.x to version 2.x** **BIOS_H12SST-1B45_20250120_3.1_STDsp.zip** **B. Package for upgrade BIOS from version 1.x to version 2.0 or above** **BIOS_H12SST-1B45-UP_20250120_3.1_STDsp.zip** **Important Notes:** **1) BIOS R 2.x supports 7002 and 7003 processors.** **2) The Flash Utility included in the package only supports updating BIOS from R1.x to R 2.x or withing R.2 versions. Rolling back is not allowed.** **3) BIOS R 2.x requires the latest motherboard CPLD before updating. If you purchased the system before March 13, 2021, please contact Supermicro Technical Support for verification before updating the BIOS.** **4) The default R2.x BIOS boot mode has been changed to EFI. If your OS is legacy, after upgrading to R2.x., please press the <Del> key during POST to enter the BIOS settings page and change the boot mode.** **5) In the event of a BIOS rescue failure, please restore your previous BIOS version by placing it on your boot drive for recovery, or initiate the recovery through the IPMI WebUI.**
Enhancements	**1. Updated AMI Modules based on 5.14_RomeCrb_0ACMK033.** **2. Updated AGESA MilanPI to version 1.0.0.E based on 5.22_MilanCrb_0ACOU028.** **3. Updated SA50289 (TianoCompress Privilege Escalation Vulnerability).** **4. Updated AMI Modules based on 5.14_RomeCrb_0ACMK034.**

	5. Updated AMI Modules based on 5.22_MilanCrb_0ACOU029.
New features	**N/A**
Fixes	**N/A**

Release Notes from Previous Release(s)

3.0 (7/29/2024)

1. Filled the DUID with the UUID to prevent all systems from having the same DUID in IPv6 DHCP.
2. Updated AMI modules based on 5.14_RomeCrb_0ACMK031.
3. Updated AMI modules based on 5.14_RomeCrb_0ACMK032.
4. Added USB IAD device class, subclass, and protocol support for ECM RNDIS.
5. Updated AGESA MilanPI to version 1.0.0.D based on 5.22_MilanCrb_0ACOU027.

2.9 (5/24/2024)

6. Updated SA50230_Supplement (Image Parser Corruption Vulnerability).
7. Updated secure boot KEK and DB (Fellow EagleStream SVN 2926).
8. Updated AMI Modules based on 5.14_RomeCrb_0ACMK029.
9. Updated AMI Modules based on 5.14_RomeCrb_0ACMK030.
10. Allowed ASPM in ACPI FACP to be enabled when PCIe ASPM is enabled.
11. Added support for AMI Resizable BAR.
12. Updated AMI Modules based on (BETA)5.22_MilanCrb_0ACOU025.
13. Implemented a feature to set the Chassis type in SMBIOS to the default value (0x11) when the Chassis type from FRU is 0x00, 0xFF, or NULL.
14. Resolved the issue with automated PXE boot OS installation.
15. Fixed "Check Secure Encrypted Virtualization Function" failure that occurred in projects that are not ROT.

2.8 (3/1/2024)

1. Updated MilanPI AGESA to 1.0.0.B based on 5.22_MilanCrb_0ACOU023.
2. Updated RomePI AGESA to 1.0.0.H based on 5.14_RomeCrb_0ACMK028.
3. Updated Milan SEV FW version from 1.37.7 to 1.37.10 for AMD-SN-3005: AMD INVD Instruction Security Notice.
4. Updated SA50216_Supplement (LogoFAIL Vulnerability).
5. Disabled "Correctable/Non-Fatal error reporting enable" bits when the BIOS item "PCI AER support" was set Disabled.
6. Updated SA50218_Supplement (Vulnerabilities in EDK2 NetworkPkg).
7. Updated AGESA MilanPI to 1.0.0.C based on 5.22_MilanCrb_0ACOU024.
8. Updated SA50230_Supplement (Image Parser Corruption Vulnerability).
9. Disabled ASPM in ACPI FACP when pcie ASPM was disabled.
10. Added support for changing PXE from UEFI(U)/Legacy(L) to L/U through Redfish.
11. Resolved an issue where the system would reboot during a flash BIOS with the watchdog function enabled.
12. Resolved the issue of MP1(SMU) and CPU WDT uncorrectable error not generating an event log.
13. Resolved the issue of where a memory multi-bit error was incorrectly reported as a correctable error.
14. Resolved the issue of failing to update SMBIOS Type 2 priority via SuperEdit.
15. Adjusted RDIMM\LRDIMM\3DSDIMM memory throttling trip-point to 85°C.
16. Resolved compatibility issues between some dmivar settings and AMI SMBIOS settings.

2.6a (9/28/2023)

1. Updated Milan B0/B1/B2 stepping CPU microcode and Milan-X B2 stepping CPU microcode for AMD-SB-7005 Security Bulletin to address the CVE-2023-20569 issue. The Milan microcodes

include B0 Milan microcode 0x0A001079, B1 Milan microcode 0x0A0011D1, and B2 Milan-X microcode 0x0A001234.
2. Added support for the Supermicro System LockDown feature.
3. Updated Rome B0 stepping CPU microcode 0x0830107A for AMD-SB-7008 Security Bulletin to address the CVE-2023-20593 issue.
4. Added a Rocky Linux Boot Option Name.
5. Restored SMCI secure boot keys and Update Secure Boot DB variables.
6. Fixed issue where the PCIe Link Width of AOC-SLG4-2H8M2 was being downgraded to x4.

2.6 (4/14/2023)

1. Updated AGESA MilanPI to 1.0.0.A based on 5.22_MilanCrb_0ACOU021 for AMD-SB-1032.
2. Removed "Vendor Keys" from Security page.
3. Changed “SMCI” to “Supermicro” in string names.
4. Updated the DBX file to fix the Secure Boot Bypass issue.
5. Updated AGESA RomePI to 1.0.0.F based on 5.14_RomeCrb_0ACMK026 for AMD-SB-1032.
6. Updated Milan B0/B1/B2 stepping CPU microcodes (B0 Milan microcode 0x0A001078, B1 Milan microcode 0x0A0011CE, and B2 Milan-X microcode 0x0A001231), and Milan-X B2 stepping CPU microcode (B2 Milan-X microcode 0x0A001231) to patch for Errata 1304, 1310, 1311, 1313, 1329, 1330, 1336, 1343, 1350, 1352, 1361, 1378,1379, 1381, 1386, 1407, 1433, and 1450.
7. Added support for FSRM and ERMSB items ONLY on motherboards installed with AMD EPYC 7003 Series processors.
8. Modified to sync the chassis type from FRU0 to SMBIOS Type 03 only on H12 models based on the SMBIOS template.
9. Removed "AMI Graphic Output Protocol Policy" from Advance page.
10. Improved the issue with the error/warning messages from dmidecode after modification.
11. Modified the GetVariable() service for buffer overflow in certain cases.

2.4 (4/19/2022)

1. Changed BIOS revision to 2.4.
2. Added setup item, "ASPM Support" in PCIe/PCI/PnP Configuration Page.
3. Added "Factory Mode" function for Production test.
4. Updated AGESA RomePI to 1.0.0.D.
5. Updated Rome B0 stepping CPU microcode 0x08301055 to patch Errata 1161, 1176, 1179, 1183, 1214, 1268, 1386, 1417.
6. Updated AGESA MilanPI to 1.0.0.8.
7. Updated Milan B0/B1/B2 stepping CPU microcode and Milan-X B2 stepping CPU microcode to patch for Errata 1304, 1310, 1311, 1313, 1329, 1330, 1336, 1343, 1350, 1352, 1361, 1378, 1379, 1381, 1386, 1407, 1415.B0 Milan microcode 0x0A001058, B1 Milan microcode 0x0A001173, B2 Milan-X microcode 0x0A001229.
8. Added setup item, "SNP Memory (RMP Table) Coverage" and "Amount of Memory to Cover" in CPU Configuration Page.

2.3a (1/25/2022)

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".
12. Fixed an issue where SUM cannot modify AMD CBS settings.
13. Fixed an issue where the SEV feature can't enable on ROT enabled MB.
14. Fixed an issue that hangs system with a TPM issue.

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