BIOS Release Notes Form

Product Name	**H12DST-B**
Release Version	**3.0**
Release Date	**7/29/2024**
Build Date	**7/29/2024**
Previous Version	**2.8**
Update Category	**Recommended**
Dependencies	**N/A**
Important Notes	**BIOS Image:** **BIOS_H12DSTB-1B3A_20240729_3.0_STDsp.bin** **BIOS Update Package:** **A. Package for upgrading BIOS from version 2.x to version 2.x** **BIOS_H12DSTB-1B3A_20240729_3.0_STDsp** **B. Package for upgrading BIOS from version 1.x to version 2.0 or above** **BIOS_H12DSTB-1B3A-UP_20240729_3.0_STDsp.zip** **Notes:** **1) BIOS R 2.x supports 7002 and 7003 processors.** **2) Flash Utility in the package supports BIOS update from R1.x to R 2.x or R2.x to R2.x only, and rolling back is not allowed.** **3) BIOS R 2.x requires the latest motherboard CPLD before updating. If you purchased the system before October 1, 2020, 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 you have a legacy OS, please press the <Del> key during POST to enter the BIOS setting to change boot mode after upgrading to R2.x.** **5) In the event of a BIOS rescue failure, please use your previous version of BIOS saved in your boot drive to boot or you could recover it through the IPMI WebUI.**
Enhancements	**1. [Rome][Milan][Enhancements] Fill DUID with UUID to avoid all system's DUID in IPv6 DHCP is the same.** **2. [Rome][Enhancements] Update AMI Modules based on 5.14_RomeCrb_0ACMK031.** **3. [Rome][Enhancements] Update AMI Modules based on 5.14_RomeCrb_0ACMK032.**

	4. [Rome][Milan][Enhancements] For UsbBus.c Add USB IAD device class/subclass/protocol support for ECM RNDIS. **5. [Milan][Enhancements] Update AGESA MilanPI to 1.0.0.D based on 5.22_MilanCrb_0ACOU027.** **6. [Rome][Milan][Enhancements] Update SA50235_Supplement(Extended Image Parser Corruption Vulnerability) to address** **01. BRLY-LOGOFAIL-2023-013(Score 5.1)** **02. BRLY-LOGOFAIL-2023-014(Score 4.4)** **03. BRLY-LOGOFAIL-2023-015(Score 4.4)** **04. BRLY-LOGOFAIL-2023-016(Score 7.5)** **05. BRLY-LOGOFAIL-2023-017(Score 7.5)** **06. BRLY-LOGOFAIL-2023-018(Score 7.5)** **07. BRLY-LOGOFAIL-2023-019(Score 7.5)** **08. BRLY-LOGOFAIL-2023-020(Score 7.5)** **09. BRLY-LOGOFAIL-2023-021(Score 4.1)** **10. BRLY-LOGOFAIL-2023-022(Score 7.5)** **11. BRLY-LOGOFAIL-2023-023(Score 7.5)** **12. BRLY-LOGOFAIL-2023-024(Score 7.5)** **7. [Rome][Milan][Enhancements] Update secure boot KEK and DB (Fellow EagleStream SVN 2926).** **8. [Rome][Enhancements] Update AMI Modules based on 5.14_RomeCrb_0ACMK029.** **9. [Rome][Enhancements] Update AMI Modules based on 5.14_RomeCrb_0ACMK030.** **10. [Rome][Milan][Enhancements] Add AMI Resizable BAR support.** **11. [Rome][Milan][Enhancements] Enable ASPM in ACPI FACP when pcie ASPM is enabled.** **12. [Rome][Milan][Enhancements] Add SMC Debug log support.** **13. [Milan][Enhancements] Update AMI Modules based on (BETA)5.22_MilanCrb_0ACOU025.** **14. [Milan][Enhancements] Add SMC_OS_PERFORMANCE_ENHANCE item** **15. [Rome][Milan][Enhancements] Set Chassis type in smbios to default (0x11) when Chassis type from fru is 0x00 or 0xFF or NULL.** **16. [Rome][Enhancements] Fix "Check Secure Encrypted Virtualization Function" fail(Projects that are not ROT will encounter problems).**
New features	**N/A**
Fixes	**1. [Rome][Milan][Fixes] Automated PXE boot OS install issue.**

Release Notes from Previous Release(s)

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 the issue of MP1(SMU) and CPU WDT uncorrectable error not generating an event log.
12. Resolved the issue of where a memory multi-bit error was incorrectly reported as a correctable error.
13. Resolved the issue of failing to update SMBIOS Type 2 priority via SuperEdit.
14. Adjusted RDIMM\LRDIMM\3DSDIMM memory throttling trip-point to 85°C.
15. Resolved compatibility issues between some dmivar settings and AMI SMBIOS settings.

2.6b (9/27/2023)

1. Restored SMCI secure boot keys and the Update Secure Boot DB variable.

2.6a (8/01/2023)

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, including 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 the name to Rocky Linux Boot Option.
5. Fixed issue with the LAN MAC address was not correctly displayed with X710 on BMC web.
6. Fixed issue with that the PCIe Link Width of AOC-SLG4-2H8M2 was downgraded to x4.

2.6 (4/13/2023)

1. Updated MilanPI to 1.0.0.A based on 5.22_MilanCrb_0ACOU021 for AMD-SB-1032.
2. Updated Milan B0/B1/B2 stepping CPU microcode and Milan-X B2 stepping CPU microcode to patch Patch for Errata 1304, 1310, 1311, 1313, 1329, 1330, 1336, 1343, 1350, 1352, 1361, 1378,1379, 1381, 1386, 1407, 1433, 1450, B0 Milan microcode 0x0A001078, B1 Milan microcode 0x0A0011CE, and B2 Milan-X microcode 0x0A001231.
3. Added support for FSRM and ERMSB. (Only available on models with AMD EPYC™ 7003 (Milan), not AMD EPYC™ 7002 (Rome). PI 1009 change default enable (Auto).)
4. Followed the SMBIOS template to sync the chassis type from FRU0 to SMBIOS Type 03 for H12 series models only.
5. Enhanced the solution for the error/warning messages from dmidecode after modification.
6. Updated AGESA RomePI to 1.0.0.F based on 5.14_RomeCrb_0ACMK026 for AMD-SB-1032.
7. Removed "AMI Graphic Output Protocol Policy" in Advanced page.

8. Modified GetVariable() service for buffer overflow in certain cases.

2.5 (9/23/2022)

1. Updated AGESA MilanPI to 1.0.0.9 based on 5.22_MilanCrb_0ACOU020.
2. Removed "Vendor Keys" in security page.
3. Modified string naming from SMCI to Supermicro.
4. Updated DBX file to fix Secure Boot Bypass issue.
5. Updated AGESA RomePI to 1.0.0.E basedd on 5.14_RomeCrb_0ACMK025

2.4a (6/2/2022)

1. Changed BIOS revision to 2.4a.
2. Fixed NVMe at Gen3 (only on AS - 2124BT-HNTR, based on system PM request.)

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.
9. Fixed incorrect RSC-PR-6-X2 riser name in the BIOS.

2.3 (10/20/2021)

1. Changed BIOS revision to 2.3.
2. Updated AGESA RomePI to 1.0.0.C.
3. Enabled Setup item: "Enhanced Preferred IO Mode".
4. Updated AGESA MilanPI to 1.0.0.6.
5. Updated Milan B0/B1 stepping CPU microcode and Milan-X B2 stepping CPU microcode to patch Erratum #1381. Processor May Hang When Coherency Probe Hits Instruction Cache Line While Evicted.
   B0 Milan microcode 0x0A00104C,
   B1 Milan microcode 0x0A001143,
   B2 Milan-X microcode 0x0A001223.
6. Patched BMC Redfish, to fix issued where the Host Interface was named “ethX” when CDN was disabled under Linux OS.
7. Disabled Legacy/EFI iSCSI support.
8. Enabled the following Setup items: "BankGroupSwapAlt", "SEV-SNP Support", "Enhanced Preferred IO Mode" and "Root Complex 0x00~0xE0 LCLK Frequency".

9. Changed default for "Wait For "F1" If Error" to Disabled

2.2 (8/31/2021)

1. Changed BIOS revision to 2.2.
2. Added Redfish/SUM Secure Boot feature and updated OOB for secure boot and reserve key.
3. Added support for SUM upload/deletion of HTTPS TLS certificate (default enabled by TOKEN "Sum_UploadTlsKey_SUPPORT").
4. Set Relaxed Ordering default to Enabled.
5. Updated AGESA MilanPI to 1.0.0.4.
6. Updated A010 GN B0 microcode 0A001046, A011 GN B1 microcode 0A001137, and A012 GN B2 microcode 0A00121D.
7. Fixed inability of SUM to modify AMD CBS settings.
8. Fixed inability to get SIOM LAN AOC-MH25G-m2S2T Mellanox MAC address.
9. Corrected RSC-PR-6-X2 riser name in BIOS

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. Added Redfish/SUM Secure Boot feature and updated OOB for secure boot and reserve Key.
5. Removed legacy iSCSI support of H12 BIOS.
6. Added force next boot to UEFI Shell support.
7. Updated AGESA MilanPI to 1.0.0.2.
8. Updated A011 GN B1 microcode 0A00111D.
9. Updated USB OC pin mapping to follow motherboard design.

2.0 (2/22/2021)

1. Changed BIOS revision to 2.0.
2. Updated AGESA to 1.0.0.1 for next generation processors.
3. Updated A011 GN B1 microcode 0A001119.
4. Updated AGESA RomePI to 1.0.0.A.
5. Fixed problem of BIOS initialization showing IPV6 address when IPV6 is disabled in the IPMI GUI.
6. Enhanced SMBIOS Type39 System Power Supply information.
7. 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.

1.2 (9/16/2020)

1. Changed BIOS revision to 1.2.
2. Updated AGESA RomePI to 1.0.0.8.
3. Updated 8310 SSP-B0 microcode 8301038.
4. Added SMCI HDD Security feature.
5. Updated help string of item "Input the description".
6. Set GPIO 108 output to high and internal pull to high.
7. Displayed "Relaxed Ordering" setup item and set to disabled by default.
8. 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).

9. Removed "$SMCUNHIDE$" string from "PCI AER support" setup item help string.
10. Added AMD IOMMU patch code to fix NVMe Devices drop and Hardware error in RH 7.x.
11. Fixed problem of TCG admin password reverting.
12. Fixed problem of "Update IPMI LAN Configuration" staying set to Yes when "IPv6 support" setup item is disabled.
13. Corrected CPU speed information in BIOS setup.
14. Fixed failure of Mellanox CX6 of AOC-MIBE6-m1CM to fill in VPD data to Type 40.

1.1 (1/10/2020)

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 patch to support AOC-M25G-i2S PXE boot.
5. Fixed issue of system hanging at post code A7h.
6. Fixed inability of SUM to change the function of NUMA Node Per Socket.

1.0b (12/12/2019)

1. Updated BIOS version to 1.0b.
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. Updated type 9 for SIOM slot to 1 base.
10. Displayed "Preferred IO" item.
11. Updated ASPEED VBIOS to version 1.09.00.
12. Added item "4-link xGMI max speed" to NB Configuration.
13. Set the de-emphasis as -2.18 for SATA port 0-5 for BPN-ADP-6SATA3H4-1UB and BPN-SAS3-217BHQ-N4 SKU.
14. Fixed problem of BIOS logging ECC error as "Multi Bit ECC Memory Error" when system generates ECC error log.
15. Fixed inability to create SLIC table after flashing OA2 with automation process.
16. Fixed inability of SUM to preserve "Common" BIOS configuration setting after flashing BIOS.
17. Fixed problem of NumLock/CapsLock/ScrollLock state clearing when user sends any key via Console redirection.
18. Fixed failures of memory frequency and data fabric memory frequency to match and performance to match expected result.
19. Added some AMD CBS items to CPU Configuration, NB Configuration, and ACPI Settings pages.
20. Added item "DF Cstates" to NB configuration page.
21. Hid items "APCB Version", "APOB Version", and "APPB Version".
22. Fixed inability of IPMI command to change boot option order for UEFI USB key.
23. Updated riser card string for auto testing.
24. Fixed inability of BMC WebGUI to display hardware information.

25. Corrected M.2 to "M.2-HC CPU1 PCI-E 3.0 X4" and SIOM to SIOM: CPU1 PCI-E 4.0 X16+X1 of Type 9 slot information.
26. Corrected the DIMM location of IPMI "Memory Device Disabled".
27. Fixed failure to restore boot priority to the default setting after flashing BIOS.
28. Fixed "SMBIOS preservation" item.
29. Fixed problem of the type 40 data maps to type 41 as unknown if the instance is larger than 1.
30. Fixed problem of the HD Audio test of WHQL HLK with Windows Server 2019 detecting System Audio device existence to verify audio WHQL.
31. Prevented display of any AMD memory error messages during the POST phase.
32. Fixed malfunction of recovery.
33. Added support for OOB SATA HDD information and asset information of 2 SATA controllers.
34. Fixed missing screen output when Boot Mode is changed to EFI.
35. Fixed the issue of "SMCI POST Screen Message" appearing on BIOS setup menu.
36. Fixed the issue of "SMCI POST Screen Message" appearing on POST screen when executing EFI Shell application.
37. Set PCIe bifurcation to x4x4x4x4 for AOC-SLG3-2M2.

1.0 (8/16/2019)
Initial Release