BIOS Release Notes Form

Product Name	**H12DSU-IN**
Release Version	**2.9**
Release Date	**05/24/2024**
Build Date	**05/24/2024**
Previous Version	**2.8**
Update Category	**Recommended**
Dependencies	**03.10.42**
Important Notes	**BIOS Image:** **BIOS_H12DSU-1B54_20240524_2.9_STDsp.bin** **BIOS Update Package:** **BIOS_H12DSU-1B54_20240524_2.9_STDsp.zip** **A. Package for upgrade BIOS from version 2.x to version 2.x** **BIOS_H12DSU-1B54_20240524_2.9_STDsp.zip** **B. Package for upgrading the BIOS from version 1.x to version 2.0 or above** **BIOS_H12DSU-1B54_20240524_2.9_STDsp_UP.zip** **Notes:** **1) BIOS version R 2.x supports 7002 and 7003 processors.** **2) The Flash Utility in the package only supports BIOS update from version R 1.x to R 2.x, and rolling back is not allowed.** **3) The default boot mode for BIOS version R2.x has been changed to EFI. If your OS is legacy, please press the <Del> key during POST to enter the BIOS setup to change boot mode after upgrading to R2.x.** **4) When updating BIOS from version 2.1 to version 2.3a or above through SUM, don't preserve the BIOS settings because some BIOS settings are modified after version 2.3a.** **5) In the event of a BIOS rescue failure, please use your previous BIOS version and put it on your boot drive to boot, or you could recover it through the IPMI WebUI.**

Enhancements	**1. Update SA50235_Supplement(Extended Image Parser Corruption Vulnerability).** **2. Update secure boot KEK and DB (Fellow EagleStream SVN 2926).** **3. Update AMI Modules based on 5.14_RomeCrb_0ACMK029.** **4. Update AMI Modules based on 5.14_RomeCrb_0ACMK030.** **5. Add AMI Resizable BAR support.** **6. Enable ASPM in ACPI FACP when PCIe ASPM is enabled.** **7. Add SMC Debug log support.** **8. Update AMI Modules based on (BETA)5.22_MilanCrb_0ACOU025.** **9. Add SMC_OS_PERFORMANCE_ENHANCE item** **10. Set Chassis type in SMBIOS to default (0x11) when Chassis type from fru is 0x00 or 0xFF or NULL.** **11. Fix "Check Secure Encrypted Virtualization Function" fail(Projects that are not ROT will encounter problems).**
New features	**N/A**
Fixes	**1. Fix the Automated PXE boot OS install issue.**

Release Notes from Previous Release(s)

2.8 (2024/01/19)

1. Updated MilanPI to 1.0.0.B based on 5.22_MilanCrb_0ACOU023.
2. Updated AGESA RomePI 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. Added support for Gen3 JBOF in H12DSU.
5. Updated SA50216_Supplement (LogoFAIL Vulnerability).
6. Resolved the issue of MP1 (SMU) and CPU WDT uncorrectable errors not generating event logs.
7. Implemented disabling of "Correctable/Non-Fatal error reporting enable" bits when BIOS item "PCI AER support" was set to Disabled.
8. Updated SA50218_Supplement (Vulnerabilities in EDK2 NetworkPkg).
9. Updated AGESA MilanPI to version 1.0.0.C based on 5.22_MilanCrb_0ACOU024.
10. Enhanced VPD data retrieval routines for E710.
11. Updated SA50230_Supplement (Image Parser Corruption Vulnerability).
12. Disabled ASPM in ACPI FACP when PCIe ASPM was disabled.
13. Added support for changing PXE from UEFI (U)/Legacy (L) to L/U through Redfish.
14. Resolved issue where the AMD Radon PRO W7500 & W7600 VGA card were not displaying in the shell or BIOS setup menu.
15. Resolved system rebooting during flash BIOS with watchdog function enabled.
16. Rectified the software tool "run-chk-nvme-status-2.1.10.sh" to accurately display NVME device order in Linux OS.
17. Fixed PB#166330 where legacy boot could not boot into PXE.
18. Corrected memory multi-bit errors to report as correctable errors.
19. Fixed failure to update SMBIOS Type2 priority via superedit.
20. Resolved issue of mystery reboots occurring on SMC compute hosts.
21. Resolved issue with setting RDIMM\LRDIMM\3DSDIMM memory throttling trip-point at 85°C (Part II).
22. Resolved compatibility issues between certain dmivar settings and AMI SMBIOS settings.

2.6a (2023/9/28)

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.
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. Renamed an option in the list of Boot Options to “Rocky Linux.”

5. Restored Supermicro secure boot keys and the Update Secure Boot DB variable. (Note that the unknown certificate "Addtrust
6. Fixed issue where the PCIe Link Width of AOC-SLG4-2H8M2 was downgraded to x4.

2.6 (04/13/2023)

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 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.
3. Added support for FSRM and ERMSB items ONLY on motherboards installed with AMD EPYC 7003 Series processors.
4. Modified to sync the chassis type from FRU0 to SMBIOS Type 03 only on H12 models based on the SMBIOS template.
5. Fixed an issue with the error and warning messages from dmidecode.
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.

2.5 (09/14/2022)

1. Updated 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 based on 5.14_RomeCrb_0ACMK025.

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.
8. B0 Milan microcode 0x0A001058,
9. B1 Milan microcode 0x0A001173, 10. B2 Milan-X microcode 0x0A001229.
11. Added setup item, "SNP Memory (RMP Table) Coverage" and "Amount of Memory to Cover" in CPU Configuration Page.

2.3a (3/3/2022)

1. Changed BIOS revision to 2.3a.

2. Added Redfish/SUM Secure Boot feature, updated 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. [Milan BIOS] Updated A010 GN B0 microcode 0A001046.
   Update A011 GN B1 microcode 0A001137.
   Update A012 GN B2 microcode 0A00121D.
6. [Milan BIOS] Updated AGESA MilanPI to 1.0.0.6.
7. [Rome BIOS] Updated AGESA RomePI to 1.0.0.C.
8. [Rome BIOS] Enabled new setup item: "Enhanced Preferred IO Mode".
9. Disabled EFI iSCSI support.
10. [Milan BIOS] Enabled new setup items: "BankGroupSwapAlt", "SEV-SNP Support", "Enhanced Preferred IO Mode" and "Root Complex 0x00~0xE0 LCLK Frequency".
11. Changed default for "Wait For "F1" If Error" to Disable.
12. Updated Firmtool2 to 2.00.17 to support AMD SEV preservation on ROT enabled motherboards.
13. Fixed SEV feature that can't be enabled on ROT capable motherboard.
14. Fixed TPM system hang issue.
15. Changed default “Prepare Link for Power Down” to disabled to fix the Intel 40Gbe driver, which happens during Cburn DC on/off stress with AOC-URG4N4-i4XTS.

2.1 (5/7/2021)

1. Changed BIOS revision to 2.1.
2. Set all OPROM control items to Legacy when boot mode is set to Dual.
3. Updated AGESA MilanPI to 1.0.0.2.
4. Updated A011 GN B1 microcode 0A00111D.
5. Updated AGESA RomePI to 1.0.0.B.
6. Updated USB OC pin mapping to follow motherboard design.
7. Removed legacy iSCSI support of H12 BIOS.
8. Added force next boot to UEFI Shell support.
9. Added Redfish/SUM Secure Boot feature updated OOB for secure boot and reserve Key.
10. Fixed failure of BIOS to upload SMBIOS and BIOS-related data to BMC since VRAM was locked.
11. Enhanced rule for reading FRU data of AOC/riser card.

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.

1.3 (11/25/2020)

1. Changed BIOS revision to 1.3.
2. Updated AGESA RomePI to 1.0.0.9.
3. Updated 8310 SSP-B0 microcode 830104D.
4. Displayed some items for GPU performance tuning.

1.2 (8/10/2020)

1. Changed BIOS revision to 1.2.
2. Updated AGESA RomePI to 1.0.0.8.
3. Updated help string of item "Input the description".
4. Corrected CPU speed information in BIOS setup.

1.0a (6/10/2020)

1. Changed BIOS revision to 1.0a.
2. Added new Gen1 ID support on BPN-SAS3-119A-N12 for new backplane CPLD firmware use.

1.0 (5/18/2020) Initial Release