BIOS Release Notes Form

Product Name	**H12DSG-O-CPU**
Release Version	**2.8**
Release Date	**1/26/2024**
Build Date	**1/26/2024**
Previous Version	**2.7**
Update Category	**Recommended**
Dependencies	**N/A**
Important Notes	**BIOS Image:** **BIOS_H12DSGO-1B55_20240126_2.8_STDsp.bin** **BIOS Update Package:** **BIOS_H12DSGO-1B55_20240126_2.8_STDsp.ZIP** **Notes:** **1. BIOS R 2.x now supports the 7002 and 7003 processors. The Flash Utility in the package only supports updating BIOS from R 1.x to R 2.x, and rolling back is not allowed.** **2. DMI data CANNOT be reserved when updating BIOS from 1.x to 2.x.** **3. BIOS R2.2 (or newer versions) can only roll back to R2.1, but it cannot roll back to R2.0 due to security updates.**
Enhancements	**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. Updated SA50216_Supplement (LogoFAIL Vulnerability).** **5. Fixed the issue where MP1 (SMU) and CPU WDT uncorrectable errors were not logged in event logs.** **6. Fixed the issue where the "Correctable/Non-Fatal error reporting enable" options were disabled when the "PCI AER support" option was set to Disabled.** **7. Updated SA50218_Supplement (Vulnerabilities in EDK2 NetworkPkg).** **8. Updated AGESA MilanPI to 1.0.0.C based on 5.22_MilanCrb_0ACOU024.** **9. Updated SA50230_Supplement (Image Parser Corruption Vulnerability).**

	10. Disabled ASPM in ACPI FACP when PCIe ASPM was disabled. **11. Supported changing Pxe from Uefi(U)/Legacy(L) to L/U through Redfish.**
New features	**N/A**
Fixes	**1. Fixed the problem that the AMD Radon PRO W7500 & W7600 VGA cards cannot be displayed in the shell or BIOS setup menu.** **2. Fixed the issue where a memory multi-bit error was reported as a correctable error.** **3. Fixed the issue with checking or updating SMBIOS Type 2 priority via SuperEdit failing.** **4. Set RDIMM/LRDIMM/3DSDIMM memory throttling trip-point at 85°C (Part II).** **5. Fixed some DMIVars not fitting with AMI SMBIOS settings.**

Release Notes from Previous Release(s)

2.7 (9/21/2023)

1. Updated Milan B0/B1/B2 stepping CPU microcode and Milan-X B2 stepping CPU microcode for AMD-SB-7005 Security Bulletin to address CVE-2023-20569 issue. B0 Milan microcode 0x0A001079, B1 Milan microcode 0x0A0011D1, 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 CVE-2023-20593 issue.
4. Added Rocky Linux Boot Option Name.
5. Updated AGESA MilanPI to 1.0.0.B based on 5.22_MilanCrb_0ACOU022.
6. Updated AGESA RomePI to 1.0.0.G based on 5.14_RomeCrb_0ACMK027.
7. Fixed issue in which the PCIe Link Width of AOC-SLG4-2H8M2 was downgraded to x4.

2.5 (11/2/2022)

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 the DBX file to fix the Secure Boot Bypass issue.
5. Updated AGESA RomePI to 1.0.0.E based on 5.14_RomeCrb_0ACMK025.

2.4 (4/22/2022)

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 (1/26/2022)

1. Changed BIOS revision to 2.3a.
2. Disabled ASPM.
3. Fixed the BIOS version, it did not match the version in the IPMI webUI.

2.3 (10/21/2021)

1. Changed BIOS revision to 2.3.
2. Updated AGESA RomePI to 1.0.0.C.
3. Exposed Setup item "Enhanced Preferred IO Mode".
4. Updated AGESA MilanPI to 1.0.0.6.

5. Patched case of BMC Redfish Host Interface being named ethX when CDN is disabled under Linux OS.
6. Disabled EFI iSCSI support.
7. Exposed Setup items "BankGroupSwapAlt", "SEV-SNP Support", "Enhanced Preferred IO Mode", and "Root Complex 0x00~0xE0 LCLK Frequency".
8. Changed default of "Wait For "F1" If Error" to Disable. Updated B0 Milan microcode 0x0A00104C, B1 Milan microcode 0x0A001143, and B2 Milan-X microcode 0x0A001223 to patch Erratum #1381 problem of processor hanging when coherency probe hits instruction cache line while evicted.

2.2 (7/31/2021)

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, A012 GN B2 microcode 0A00121D, and AGESA RomePI to 1.0.0.C.
7. Fixed inability of SUM to modify AMD CBS settings.
8. Fixed missing sensor information on IPMI WebGUI.

2.1 (5/10/2021)

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 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. Fixed problem of BIOS recovery occurring when using AFU to clear event log and then AC cycles the system.

2.0 (3/12/2021)

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. 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. Disabled USB OC feature.
8. Fixed inability to use F12 hotkey to boot into PXE.
9. Fixed inability to detect AMD GPU cards on Slot7.

1.3 (12/18/2020)

1. Changed BIOS revision to 1.3.
2. Updated AGESA RomePI to 1.0.0.9.
3. Updated 8310 SSP-B0 microcode 0830104D.

4. 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.

1.2a (11/19/2020)

1. Changed BIOS revision to 1.2a.
2. Fixed inability of the BIOS to boot to OS/UEFI Shell in assembly house.

1.2 (9/24/2020)

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. Added support for different system configurations.
5. Removed Marvell 9230 OPROM from BIOS.
6. Updated SMBIOS type 42 data for IPMI Redfish Host Interface support.
7. Corrected CPU speed information in BIOS setup.

1.0 (5/26/2020)

Initial Release