BIOS Release Notes Form

Product Name	**H12DSi-N6/NT6**
Release Version	**3.3**
Release Date	**3/28/2025**
Previous Version	**3.0**
Update Category	**Recommended**
Dependencies	**IPMI FW 01.06.01**
Important Notes	**BIOS Image:** **BIOS_H12DSI-1C22_20250328_3.3_STDsp.bin** **BIOS Update Package:** **BIOS_H12DSI-1C22_20250328_3.3_STDsp.zip**
Enhancements	**1. Updated AMI Modules based on 5.14_RomeCrb_0ACMK033.** **2. Updated AGESA MilanPI to 1.0.0.E based on 5.22_MilanCrb_0ACOU028.** **3. Updated SA50289(TianoCompress Privilege Escalation Vulnerability) to address CVE-119.** **4. Updated AMI Modules based on 5.14_RomeCrb_0ACMK034.** **5. Updated AMI Modules based on 5.22_MilanCrb_0ACOU029.** **6. Updated AMI Modules based on 5.14_RomeCrb_0ACMK035.** **7. Updated Legacy Serial Redirection module from MAINT_LegacySreDir_13.01 to MAINT_LegacySreDir_14.01.** **8. Updated AMI Modules based on 5.22_MilanCrb_0ACOU030.** **9. Updated Secure Boot DBX to address AMI SA50300 (CVE-2024-7344\CVE-2023-24932 (8.2 High/6.7 Middle)) security issue.**
New features	**N/A**
Fixes	**N/A**

Release Notes from Previous Release(s)

3.0 (7/29/2024)

1. Filled DUID with UUID to avoid DUID in IPv6 DHCP being the same in all systems.
2. Updated AMI modules based on 5.14_RomeCrb_0ACMK031.
3. Updated AMI modules based on 5.14_RomeCrb_0ACMK032.
4. For UsbBus.c, added USB IAD device class/subclass/protocol support for ECM RNDIS.
5. Updated AGESA MilanPI to 1.0.0.D based on 5.22_MilanCrb_0ACOU027.

2.9 (5/29/2024)

1. Updated 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)
2. Updated secure boot KEK and DB (Fellow EagleStream SVN 2926).
3. Fixed HostInterface On/Off test dropping 4x times in UEFI Shell.
4. Updated AMI Modules based on 5.14_RomeCrb_0ACMK029.
5. Updated AMI Modules based on 5.14_RomeCrb_0ACMK030.
6. Added AMI Resizable BAR support.
7. Enabled ASPM in ACPI FACP when PCIe ASPM is enabled.
8. Added SMC Debug log support.
9. Updated AMI Modules based on 5.22_MilanCrb_0ACOU025.
10. Added SMC_OS_PERFORMANCE_ENHANCE item.
11. Set chassis type in SMBIOS to default (0x11) when chassis type from fru is 0x00 or 0xFF or NULL
12. Automated PXE boot OS install issue.

2.8 (2/27/2024)

1. Updated AGESA 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 MP1(SMU) and CPU WDT uncorrectable error no event log issue.
6. Disabled "Correctable/Non-Fatal error reporting enable" bits when BIOS item "PCI AER support" is 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 is disabled
11. Fixed the problem where the AMD Radon PRO W7500 & W7600 VGA card cannot be displayed in the shell or BIOS setup menu.
12. Fixed memory multi-bit error being reported as a correctable error.

13. Checked Update SMBIOS Type2 priority via superedit fail.

2.7 (10/25/2023)

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. Support for 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. Restored SMCI secure boot keys and Updated Secure Boot DB variable.
6. Updated MilanPI to 1.0.0.B based on 5.22_MilanCrb_0ACOU022.
7. Updated AGESA RomePI to 1.0.0.G based on 5.14_RomeCrb_0ACMK027.
8. Support for changing Pxe from Uefi(U)/Legacy(L) to L/U through Redfish.
9. Fixed PCIe Link Width of AOC-SLG4-2H8M2 downgraded to x4.
10. Set RDIMM\LRDIMM\3DSDIMM memory throttling trip-point at 85C part II.
11. Fixed some dmivar unfit with ami smbios settings.

2.6 (4/13/2023)

1. Removed "Vendor Keys" on security page.
2. Modified String naming from SMCI to Supermicro.
3. Updated DBX file to fix Secure Boot Bypass issue.
4. Updated MilanPI to 1.0.0.A based on 5.22_MilanCrb_0ACOU021 for AMD-SB-1032.
5. 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, 1433, 1450.
   29126B0 Milan microcode 0x0A001078,
   B1 Milan microcode 0x0A0011CE,
   B2 Milan-X microcode 0x0A001231.
6. Followed the SMBIOS template to sync the chassis type from FRU0 to SMBIOS Type 03 (only for H12 projects).
7. Updated AGESA RomePI to 1.0.0.F based on 5.14_RomeCrb_0ACMK026 for AMD-SB-1032.
8. Added FSRM and ERMSB items support. (Milan only, Rome not supported. PI 1009 changed default to enabled (Auto).
9. [SecurityErase] Modified GetVariable() service for buffer overflow in certain cases.

2.4 (4/22/2022)

1. Changed BIOS revision to 2.4.
2. Added setup item, "ASPM Support" to PCIe/PCI/PnP Configuration Page.
3. Added "Factory Mode" function to 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" to CPU Configuration Page.

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.
9. 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.
10. Added Redfish/SUM Secure Boot feature and updated OOB for secure boot and reserve Key.
11. Added support for SUM upload/delete HTTPS TLS certificate (Default Enabled by TOKEN "Sum_UploadTlsKey_SUPPORT").
12. Set Relaxed Ordering default to Enabled.
13. Set all OPROM control items to Legacy when boot mode is set to Dual.
14. Removed legacy iSCSI support of H12 BIOS.
15. Added force next boot to UEFI Shell support.
16. Fixed missing sensor information on IPMI WebGUI.
17. Fixed problem of AFU being used to clear event log and then AC cycling the system after BIOS recovery.

2.0 (4/09/2021)

Initial Release