BIOS Release Notes Form

Product Name	**H12SSW-iN/NT (All)**
Release Version	**2.8**
Release Date	**01/16/2024**
BIOS Date	**01/16/2024**
Previous Version	**2.7**
Update Category	**Recommend**
Dependencies	**N/A**
Important Notes	**ECO #29476** **BIOS image: BIOS_H12SSW-1B2B_20240116_2.8_STDsp.bin** **Please update BIOS with attached Flash Utility in package.**
Enhancements	1. Update MilanPI to 1.0.0.B based on 5.22_MilanCrb_0ACOU023. 2. Update AGESA RomePI to 1.0.0.H based on 5.14_RomeCrb_0ACMK028. 3. Update Milan SEV FW version from 1.37.7 to 1.37.10 for AMD-SN-3005: AMD INVD Instruction Security Notice. 4. Asmedia USB controller PEI recovery support; None of the four back-end USB ports of the H12SSWL/H12SSW system can detect the recovery image(SUPER.ROM) 5. Update SA50216_Supplement(LogoFAIL Vulnerability).An attacker can exploit this vulnerability by flashing firmware containing a maliciously-crafted logo image and booting this system with the altered image. On devices vulnerable to LogoFAIL, attackers can supply custom logos and thus exploit any vulnerabilities in the image parser. This weakness affects a variety of image formats including GIF, PNG, BMP and JPEG. 6. Fixed MP1(SMU) and CPU WDT uncorrectable error no event log issue. 7. Disable "Correctable/Non-Fatal error reporting enable" bits when BIOS item "PCI AER support" set Disabled. 8. Update SA50218_Supplement(Vulnerabilities in EDK2 NetworkPkg). 9. Update AGESA MilanPI to 1.0.0.C based on 5.22_MilanCrb_0ACOU024. 10. Update SA50230_Supplement(Image Parser Corruption Vulnerability). 11. Disable ASPM in ACPI FACP when pcie ASPM is disabled. 12. 1.Set offset 0x46 value of MP2855(slave address 0x40) to 0xB8B4; Adjust OCP_TDC from 288A to 360A. 2.Set offset 0x47 value of MP2855(slave address 0x40) to 0x7F00; Adjust trigger delay to 0 ms and action delay to 31 us 3.Set offset 0x49 value of MP2855(slave address 0x40) to 0xCC36; Adjust OCP_PHASE_LIMIT from 45A(315A) to 54A(378A)
New features	N/A

Fixes	1. Fixed System would reboot during flash BIOS with watchdog function enable. 2. Fixed SUM GetSataInfo Fail 3. Fixed memory multi-bit error will report to correctable error. 4. Check Update SMBIOS Type2 priority via superedit fail.

Release Notes from Previous Release(s)

2.7 (10/25/2023)

1. [Milan] Update AGESA MilanPI to 1.0.0.B.
2. [Rome] Update AGESA RomePI to 1.0.0.G.
3. [Milan][Rome][SmcOptIpmiBoot][Enhancements] Support that changing Pxe from Uefi(U)/Legacy(L) to L/U through Redfish; It can adjust setup option and priority of Pxe boot order according to Boot Flag Command.
4. [Milan][Rome] Fixes when Set RDIMM\LRDIMM\3DSDIMM memory throttling trip-point @85C part II.
5. [Milan]Fix some dmivar unfit with ami smbios settings; AMI using UnicodeSPrint instead of Swprintf. The hex number case was different.

2.6 (09/28/2023)

1. [Milan]Update 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.
2. [Rome]Update Rome B0 stepping CPU microcode 0x0830107A for AMD-SB-7008 Security Bulletin to address CVE-2023-20593 issue.
3. [Milan][Rome]Add Rocky Linux Boot Option Name.
4. [Milan][Rome]Enable token ASM1061_Workaround to disable ASM1061 64-bit memory address capability.
5. [Milan][Rome]Restore SMCI secure boot keys and Update Secure Boot DB variable. (Unknown certificate "Addtrust External CA Root" is expired on May 30th 2020).
6. [Milan][Rome][Fixes] Fixed that the PCIe Link Width of AOC-SLG4-2H8M2 is downgraded to x4.

2.5 (9/26/2022)

1. Update MilanPI to 1.0.0.9 based on 5.22_MilanCrb_0ACOU020.
2. Remove "Vendor Keys" in security page, Duplicate item in Security Page and Key Management page.Remove from security page to prevent user confuse.
3. Modify String naming from SMCI to Supermicro.
4. Update DBX file to fix Secure Boot Bypass issue. CVEs released for this issue: CVE-2020-10713(8.2, High), CVE-2022-34301(8.2, High), CVE-2022-34302(8.2, High), CVE-2022-34303(8.2, High) security issues.
5. Update AGESA RomePI to 1.0.0.E based on 5.14_RomeCrb_0ACMK025.

2.4 (4/13/2022)

1. Change BIOS revision to 2.4.
2. Exposed setup item "ASPM Support" in PCIe/PCI/PnP Configuration Page.
3. Add the "Factory Mode" function for the Production test.
4. Update AGESA RomePI to 1.0.0.D.
5. Update Rome B0 stepping CPU microcode 0x08301055 to patch Errata 1161, 1176, 1179, 1183, 1214, 1268, 1386, 1417.
6. Update AGESA MilanPI to 1.0.0.8.
7. Update Milan B0/B1/B2 stepping CPU microcode and Milan-X B2 stepping CPU microcode to patch 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. Exposed setup items "SNP Memory (RMP Table) Coverage" and "Amount of Memory to Cover" in CPU Configuration Page for SEV-SNP feature use.

2.3 (10/20/2021)

1. Change BIOS revision to 2.3.
2. Add Redfish/SUM Secure Boot feature, update OOB for secure boot, and reserve Key.
3. Support SUM upload/delete HTTPS TLS certificate. (Default Enabled by TOKEN "Sum_UploadTlsKey_SUPPORT")
4. Per AMD's suggestion, set Relaxed Ordering default to Enabled.
5. Update AGESA RomePI to 1.0.0.C.
6. Exposed Setup item "Enhanced Preferred IO Mode".
7. Update AGESA MilanPI to 1.0.0.6.
8. Update 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.
9. Patch BMC Redfish Host Interface was named as ethX when CDN was the disabled case under LinuxOS.
10. Disable Legacy/EFI iSCSI support.

11. Exposed Setup items "BankGroupSwapAlt", "SEV-SNP Support", "Enhanced Preferred IO Mode", and "Root Complex 0x00~0xE0 LCLK Frequency".
12. [Milan BIOS] Fix SUM cannot modify AMD CBS settings.

2.0 (02/22/2021)

1. Change BIOS revision to 2.0.
2. Support both AMD EPYC 7002 and next generation processors.
3. Update A011 GN B1 microcode 0A001119.
4. Update AGESA RomePI to 1.0.0.A.
5. Per Platform Management FRU Information Storage Definition v1.1 to enhance SMBIOS Type39 System Power Supply information

1.3 (11/25/2020)

1. Updated BIOS revision to 1.3.
2. Updated AGESA RomePI to 1.0.0.9.
3. Updated 8310 SSP-B0 microcode 830104D.
4. Displayed TSME, DDR Power Down Enable, and PCIe Ten Bit Support for GPU performance tuning.

1.2 (10/14/2020)

1. [Enhancements] Change BIOS revision to 1.2.
2. [Enhancements] Update AGESA RomePI to 1.0.0.8.
3. [Enhancements] Update 8310 SSP-B0 microcode 8301038.
4. [Enhancements] Add SMCI HDD Security feature.
5. [Enhancements] Per System LAB request, update help string of item "Input the description".
6. [Enhancements] Per PM's request to update M.2 strings of OPROM items and SMBIOS Type9 information.
1.[Fixes] Fixed Fru0 - Manufacturer Name (PM) doesn't sync. to SMBIOS Type 3 - Manufacturer (CM).
Fixed Fru0 - Product Part/Model Number (PPM) doesn't sync. to SMBIOS Type 1 - ProductName(PN).
2.[Fixes] Remove "$SMCUNHIDE$" string from "PCI AER support" setup item help string.
3.[Fixes] Add AMD IOMMU patch code for fixing NVME Devices drop and Hardware error in RH 7.x.
4.[Fixes] Fixed TCG admin password reverse bug.
5.[Fixes] CPU speed information in not correct in BIOS setup.
6.[Fixes] Support function disable of SATA controller for unused SATA controller of M.2 and PCIe devices.
7.[Fixes] Fixed system hang post code 95h (Out of resource) when SR-IOV setting is enabled in Setup and Broadcom 57416 OPROM.

1.1a (05/28/2020)

1. Change BIOS revision to 1.1a.
2. Update AGESA RomePI to 1.0.0.7.
3. Update 8310 SSP-B2 microcode 8301038.
4. Fix system will hang on POSTCODE 0xB2 when JPG1 set to disabled and plug-in the VGA card.
5. Add SMCI HDD Security feature.
6. Fixes the Fru0 - Manufacturer Name (PM) doesn't sync. to SMBIOS Type 3 - Manufacturer (CM).
Fixed Fru0 - Product Part/Model Number (PPM) doesn't sync. to SMBIOS Type 1 - ProductName (PN).
6. Fixes the Remove "$SMCUNHIDE$" string from "PCI AER support" setup item help string.
7. Fixes Add AMD IOMMU patch code for fixing NVME Devices drop and Hardware error in RH 7.x.
8. Fixes TCG admin password reverse bug.

1.0b (11/15/2019)

1. Change BIOS revision to 1.0b.
2. Add "DRAM Scrub Time" in Memory Configuration.
3. Update AGESA RomePI to 1.0.0.4 based on 5.14_RomeCrb_0ACMK012.
4. Use AMD CBS "PCIe ARI Support" item instead of "ARI Forwarding".
5. Update item string "Input the description" and "HTTP Boot One Time" to meet Rome BIOS Setup Template v0.7_20190705.
6. Show 3rd IPMI version in BIOS setup.
7. According to each project's board ID, update SSID of AMD Host Bridge.
8. Set IOMMU default as Auto (Enabled)
9. Exposed item "Preferred IO".
10. Do not display any AMD memory error messages during the POST phase.
11. Fixes recovery function cannot work.
12. Support OOB SATA HDD information and asset information of 2 SATA controllers.
13. No screen output when Boot Mode is changed to EFI.
14. Fixes system will hang when installing NVidia RTX 2080/5000/6000
15. Fixes the issue that "SMCI POST Screen Message" might be shown on BIOS setup menu.
16. Fixes the issue that "SMCI POST Screen Message" might be shown on POST screen during executing EFI Shell application.
17. Patch I/O error message happened when run SPEC CPU2017 test on Asmedia SATA port HDD

Revision 1.0 (2019/07/19)

First release.