IPMI Firmware / BIOS Release Notes Form

Product Name	**H12SSW-NTR**
Release Version	**2.8**
Release Date	**02/27/2024**
Build Date	**02/27/2024**
Previous Version	**2.7**
Update Category	**Recommended**
Dependencies	**N/A**
Important Notes	**ECO #29690** **BIOS Image: BIOS_H12SSWR-1B74_20240227_2.8_STDsp.bin - BIOS image** **BIOS Update Package: BIOS_H12SSWR-1B74_20240227_2.8_STDsp.zip** **Please update BIOS with attached Flash Utility in package.**
Enhancements	1. Update MilanPI to 1.0.0.B based on 5.22_MilanCrb_0ACOU023 ; Security Update for SA50212, SA50202, SA50209, SA50198, SA50185, SA50179, SA50197, SA50219, SA50193 and SA50191. 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. 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. 5. Disable "Correctable/Non-Fatal error reporting enable" bits when BIOS item "PCI AER support" set Disabled. 6. Update SA50218_Supplement (Vulnerabilities in EDK2 NetworkPkg). Description: Quarkslab sighted seven exploitable security issues in the TianoCore EDK2 NetworkPkg which AMI integrates into Aptio V. 7. Update AGESA MilanPI to 1.0.0.C based on 5.22_MilanCrb_0ACOU024. 8. Update SA50230_Supplement (Image Parser Corruption Vulnerability). 9. Disable ASPM in ACPI FACP when pcie ASPM is disabled.
New features	N/A
Fixes	1. Fixes the SUM GetSataInfo Fail 2. Fixed MP1(SMU) and CPU WDT uncorrectable error no event log issue. 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)

Revision 2.7(10/25/2023)

1. [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).
2. [Milan] Update MilanPI to 1.0.0.B based on 5.22_MilanCrb_0ACOU022.
3. [Rome] Update AGESA RomePI to 1.0.0.G based on 5.14_RomeCrb_0ACMK027.
4. [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.
5. [Milan][Rome] Set RDIMM\LRDIMM\3DSDIMM memory throttling trip-point @85C part II, According to DDR4 Spec and our thermal design guide.
6. [Milan][Rome] Modify the reading BPNID method from BMC.fixes during the DC/AC long run test, PCIe device will not match.
7. [Milan][Rome] Fixed the issue that SUT will hang at post code "92" when AsMedia SATA Controller is Disabled.
8. [Milan]Fix some dmivar unfit with ami smbios settings, AMI using UnicodeSPrint instead of Swprintf. The hex number case was different.

Revision 2.6a(2022/10/06)

1. 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. Support the Supermicro System LockDown feature.
3. Update Rome B0 stepping CPU microcode 0x0830107A for AMD-SB-7008 Security Bulletin to address CVE-2023-20593 issue.
4. Add Rocky Linux Boot Option Name.
5. Enable token ASM1061_Workaround to disable ASM1061 64-bit memory address capability.
6. Update MilanPI to 1.0.0.A based on 5.22_MilanCrb_0ACOU021 for AMD-SB-1032.
7. Update 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.
8. Follow the SMBIOS template sync the chassis type from FRU0 to SMBIOS Type 03, only for H12 projects.
9. Update AGESA RomePI to 1.0.0.F based on 5.14_RomeCrb_0ACMK026 for AMD-SB-1032.
10. Modified GetVariable() service for buffer overflow in certain cases.
11. Fixes keep the PCIe original bifurcation when the required link width for the AOC-SLG card is greater than x4.
12. Fixes When AsMedia SATA Controller Disabled SUT will hang at post code "92"

Revision 2.5(2022/10/06)

1. Update Milan AGESA to 1.0.0.9
2. Update Rome AGESA to 1.0.0.E
3. Follow the SMBIOS template and sync the chassis type from FRU0 to SMBIOS Type 03.
4. Fixed the system can't boot to UEFI USB KEY with command 'ipmi power bootoption 11'.
5. Fixed Update SMBIOS type 41 data. Change "NEC USB" string to "Renesas USB"

Revision 2.4(2022/02/23)

1. Update Milan AGESA to 1.0.0.8
2. Update Rome AGESA to 1.0.0.D
3. Fixed the system randomly hanged postcode "0x00"/"0xCd"/"0x4b" when the system runs AC On/Off burning test.
4. Fixed the system hanged postcode "AC" when TPM 2.0 module is installed.
5. Fixed the MAC address of AOC-A25G-i2SM that can't show in BMC Web UI.
6. Fixed Milan and Milan-X CPU can't detect AMD GPU MI210 populated on slot-1 but Rome can.
7. Change each root bridge MMIO size from 16M to 64M to fix out of resource issue.

Revision 2.3 (2021/10/01)

1. Update Milan AGESA to 1.0.0.6
2. Update Rome AGESA to 1.0.0.C

Revision 2.2 (2021/08/09)

1. Followed the new cable plan to change the G1 & G2 PCIe config.
2. New AIOM card (AOC-A100G-m2CM) is Support; BIOS supports this AIOM card for BMC sensor reading.
3. When the AIOM1 changed device, the BMC gets a reset. However, it causes the BIOS cannot update the OOB file successfully.
4. Update BIOS version from 2.1 to 2.2
5. USB controller PCIe gen. speed fix from PCIe Gen. 1 to PCIe Gen. 2

Revision 2.1 (2021/07/12)

fixes the BIOS version shows incorrectly

Revision 2.0 (2021/05/25)

First release.