BIOS Release Notes Form

Product Name	**H12SSW-iNL/NTL (All)**
Release Version	**2.8**
Release Date	**01/19/2024**
BIOS Date	**01/19/2024**
Previous Version	**2.7**
Update Category	**Recommend**
Dependencies	**N/A**
Important Notes	**ECO #29805** **BIOS image: BIOS_H12SSWL-1B98_20240119_2.8_STDsp.bin** **Please update BIOS with attached Flash Utility in package.**
Enhancements	1. Update MilanPI to AGESA MilanPI to 1.0.0.C based on 5.22_MilanCrb_0ACOU024. 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. enhancement the 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 ; Make sure BIOS event log page can log 0x0B for processor error. 7. Disable "Correctable/Non-Fatal error reporting enable" bits when BIOS item "PCI AER support" set Disabled; Device Control Register (Capability ID: 0x10) Offset 08h bit[1:0] 8. Update SA50218_Supplement(Vulnerabilities in EDK2 NetworkPkg); Quarkslab sighted seven exploitable security issues in the TianoCore EDK2 NetworkPkg which AMI integrates into Aptio V. 9. Update SA50230_Supplement(Image Parser Corruption Vulnerability).When a user flashes firmware to a system containing a maliciously crafted monochrome BMP or animated GIF logo image file, the system may become unresponsive. 10. Disable ASPM in ACPI FACP when pcie ASPM is disabled.ASPM should be disabled when pcie aspm is disabled.
New features	**N/A**
Fixes	1. Fixed the problem that the AMD Radon PRO W7500 & W7600 VGA card cannot be displayed in the shell or BIOS setup menu. 2. Fixed the System would reboot during flash BIOS with watchdog function enable. 3. Fixed memory multi-bit error will report to correctable error. Added confirmation ECC type to determine what kind of error. 4. Check Update SMBIOS Type2 priority via superedit fail.The fru1 data not cover with the superedit data.

Release Notes from Previous Release(s)

Revision 2.7 (10/25/2023)
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.
B0 Milan microcode 0x0A001079, B1 Milan microcode 0x0A0011D1, B2 Milan-X microcode 0x0A001234.
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 the Secure Boot DB variable. (Unknown certificate "Addtrust External CA Root" is expired on May 30th 2020).
6. [Milan]Update MilanPI to 1.0.0.B based on 5.22_MilanCrb_0ACOU022.
7. [Rome] Update AGESA RomePI to 1.0.0.G based on 5.14_RomeCrb_0ACMK027.
8. [Milan][Rome][SmcOptIpmiBoot] Support that changing Pxe from Uefi(U)/Legacy(L) to L/U through Redfish.
9. [Milan][Rome] Fixed that the PCIe Link Width of AOC-SLG4-2H8M2 is downgraded to x4.
10. [Milan][Rome] Fixes and Set RDIMM\LRDIMM\3DSDIMM memory throttling trip-point @85C part II.
11. [Milan] Fix some dmivar unfit with ami smbios settings; AMI using UnicodeSPrint instead of Swprintf. The hex number case was different.

Revision 2.6 (04/14/2023)
1. Update MilanPI to 1.0.0.A based on 5.22_MilanCrb_0ACOU021 for AMD-SB-1032.
2. 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. B0 Milan microcode 0x0A001078, B1 Milan microcode 0x0A0011CE, B2 Milan-X microcode 0x0A001231.
3. Follow the SMBIOS template to sync the chassis type from FRU0 to SMBIOS Type 03, only for H12 projects.
4. Enhance the solution for the error/warning message from dmidecode after a modification.
5. Update AGESA RomePI to 1.0.0.F based on 5.14_RomeCrb_0ACMK026 for AMD-SB-1032.

Revision 2.4 (04/14/2022)
1. Add Redfish/SUM Secure Boot feature, update OOB for secure boot, and reserve Key.
2. Support SUM upload/delete HTTPS TLS certificate. (Default Enabled by TOKEN "Sum_UploadTlsKey_SUPPORT"); Refer Whitley SVN 3116/3114 to update SmcHttpBoot module.
3. Per AMD's suggestion, set Relaxed Ordering default to Enabled.
4. Update AGESA RomePI to 1.0.0.D.
5. Exposed Setup item "Enhanced Preferred IO Mode", By AMD's suggestion.
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.
8. Patch BMC Redfish Host Interface was named as ethX when CDN was the disabled case under Linux OS.
9. Disable Legacy/EFI iSCSI support for security concerns.
10. Exposed Setup items "BankGroupSwapAlt", "SEV-SNP Support", "Enhanced Preferred IO Mode", and "Root Complex 0x00~0xE0 LCLK Frequency" by AMD's suggestion.
11. Disable "Wait For "F1" If Error".
12. Exposed setup item "ASPM Support" in PCIe/PCI/PnP Configuration Page.
13. Add the "Factory Mode" function for the Production test.
14. Update Rome B0 stepping CPU microcode 0x08301055 to patch Errata 1161, 1176, 1179, 1183, 1214, 1268, 1386, 1417.
15. Exposed setup items "SNP Memory (RMP Table) Coverage" and "Amount of Memory to Cover" on CPU Configuration Page

Revision 2.0 (02/22/2021)
1. [Rome/Milan BIOS] Change BIOS revision to 2.0.
2. [Milan BIOS] Update AGESA MilanPI to 1.0.0.1.
3. [Milan BIOS] Update A011 GN B1 microcode 0A001119.
4. [Rome BIOS] Update AGESA RomePI to 1.0.0.A.
5. [Rome/Milan BIOS] Fix IPV6 disable in the IPMI GUI but BIOS initialize will appear IPV6 address.

Revision 1.0 (2019/07/19)
First release.