IPMI Firmware / BIOS Release Notes Form

Product Name	**H12SSW-iNR/NTR**
Release Version	**2.5**
Release Date	**09/23/2022**
Build Date	**09/23/2022**
Previous Version	**2.4**
Update Category	**Critical**
Dependencies	**N/A**
Important Notes	**ECO #27487** **BIOS_H12SSWR-1B74_20220923_2.5_STDsp.bin** **BIOS Update Package: BIOS_H12SSWR-1B74_20220923_2.5_STDsp.zip** **Please update BIOS with attached Flash Utility in package.**
Enhancements	1. Update MilanPI to 1.0.0.9 based on 5.22_MilanCrb_0ACOU020. 2. Modify String naming from SMCI to Supermicro. 3. Update DBX file to fix Secure Boot Bypass issue; Update dbxupdate_x64.bin /dbxupdate_x86.bin /dbxupdate_arm64.bin 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. 4. Update AGESA RomePI to 1.0.0.E based on 5.14_RomeCrb_0ACMK025.
New features	N/A
Fixes	N/A

Release Notes from Previous Release(s)

Revision 2.4(04/13/2022)

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 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. Exposed setup items "SNP Memory (RMP Table) Coverage" and "Amount of Memory to Cover" on the CPU Configuration Page.
9. Fixed SEV feature can't enable on ROT enabled MB.
10. Fixed that system hangs with TPM issue.

Revision 2.3 (10/28/2021)

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" by AMD's suggestion.
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.
10. Patch BMC Redfish Host Interface was named as ethX when CDN was the disabled case under Linux OS; Supported EUI-48 Locally Administered MAC Address.
11. Disable Legacy/EFI iSCSI support.
12. Exposed Setup items "BankGroupSwapAlt", "SEV-SNP Support", "Enhanced Preferred IO Mode", and "Root Complex 0x00~0xE0 LCLK Frequency".
13. Adjust the USB2.0 SWING setting when using BPN-NVME3-802N-S4 base on HW request.
14. Set BPN-NVMe3-802N-S4 to 4+0 mode for AMD platform based on HW request.
15. Exchange default setting of "Wait For "F1" If Error" to Disable.
16. Fix SUM cannot modify AMD CBS settings.
17. Patch AsMedia Keyboard not work during legacy OPROM execution.

Revision 2.1 (2021/05/07)

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 2.0 (2021/02/22)

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.Platform Management FRU Information Storage Definition v1.1 to enhance SMBIOS Type39 System Power Supply information.
6.Fixed F12 hotkey boot into PXE.
7.Fixed IPV6 disabled in the IPMI GUI but BIOS initialize will appear IPV6 address.

Revision 1.3 (2020/11/25)

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.
5. Fixed inability of the BIOS to boot to OS/UEFI Shell in assembly house.

Revision 1.2 (2020/08/26)

1. Change BIOS revision to 1.2.

2. Update AGESA RomePI to 1.0.0.8.
3. Update 8310 SSP-B0 microcode 8301038.
4. Add SMCI HDD Security feature.
5. Per System LAB request, update help string of item "Input the description".
6. Update USB Exposed port fail with WHQL testing.
7. Update hot plug setting for AS-1114S-WN10RT cable routing change.
8. 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).
9. Remove "$SMCUNHIDE$" string from "PCI AER support" setup item help string.
10. Add AMD IOMMU patch code for fixing NVME Devices drop and Hardware error in RH 7.x.
11. Fixed TCG admin password reverse bug.
12. CPU speed information in not correct in BIOS setup.
13. Fixed EFI version of PassMark MemTest86 hangs up when SMCI Redfish Host Interface disabled/un-supported in IPMI FW.

Revision 1.0 (2020/05/27)

1. First release.