IPMI Firmware / BIOS Release Notes Form

Supermicro disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade. All products, computer systems, dates, and figures specified are preliminary based on current expectations, and are subject to change without notice. Supermicro and the Supermicro logo are trademarks of Super Micro Computer, Inc. in the U.S. and/or other countries. Copyright © 2018 Super Micro Computer, Inc. All rights reserved.

Product Name	**H12SSL-i/C/CT/NT**
Release Version	**2.8**
Release Date	**02/27/2024**
Previous Version	**2.7**
Update Category	**Recommend**
Dependencies	**N/A**
Important Notes	**N/A**
Enhancements	1. [Milan][Enhancements] Update MilanPI to 1.0.0.B based on 5.22_MilanCrb_0ACOU023. 2. [Rome][Enhancements] Update AGESA RomePI to 1.0.0.H based on 5.14_RomeCrb_0ACMK028. 3. [Milan][Enhancements] Update Milan SEV FW version from 1.37.7 to 1.37.10 for AMD-SN-3005: AMD INVD Instruction Security Notice. 4. [Milan][Rome][Enhancements] Update SA50216_Supplement(LogoFAIL Vulnerability). 5. [Milan][Rome][Enhancements] Fixed MP1(SMU) and CPU WDT uncorrectable error no event log issue. 6. [Milan][Rome][Enhancements] Disable "Correctable/Non-Fatal error reporting enable" bits when BIOS item "PCI AER support" set Disabled. 7. [Milan][Rome][Enhancements] Update SA50218_Supplement(Vulnerabilities in EDK2 NetworkPkg). 8. [Milan][Enhancements] Update AGESA MilanPI to 1.0.0.C based on 5.22_MilanCrb_0ACOU024. 9. [Milan][Rome][Enhancements] Update SA50230_Supplement(Image Parser Corruption Vulnerability). 10. [Milan][Rome][Enhancements] Disable ASPM in ACPI FACP when PCIe ASPM is disabled.

New features	N/A
Fixes	1. [Milan][Rome][Fixes] Fixed the problem that the AMD Radon PRO W7500 & W7600 VGA card cannot be displayed in the shell or BIOS setup menu. 2. [Milan][Rome][Fixes] Fixed memory multi-bit error will report to correctable error. 3. [Milan][Rome][Fixes] Check Update SMBIOS Type2 priority via superedit fail.

2.7 (10/25/2023)

1. [Milan][Enhancements] Update MilanPI to 1.0.0.B based on 5.22_MilanCrb_0ACOU022.
2. [Rome][Enhancements] Update AGESA RomePI to 1.0.0.G based on 5.14_RomeCrb_0ACMK027.
3. [Milan][Rome][SmcOptIpmiBoot][Enhancements] Support that changing Pxe from Uefi(U)/Legacy(L) to L/U through Redfish.
4. [Milan][Rome][Fixes] Set RDIMM\LRDIMM\3DSDIMM memory throttling trip-point @85C part II.
5. [Milan][Fixes] Fix some dmivar unfit with ami smbios settings.

2.6a (08/01/2023)

1. [Milan][Enhancements] 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. [Milan][Enhancements] Support Supermicro System LockDown feature.
3. [Rome][Enhancements] Update Rome B0 stepping CPU microcode 0x0830107A for AMD-SB-7008 Security Bulletin to address CVE-2023-20593 issue.
4. [Milan][Rome][Enhancements] Add Rocky Linux Boot Option Name.
5. [Milan][Enhancements] Update MilanPI to 1.0.0.A based on 5.22_MilanCrb_0ACOU021 for AMD-SB-1032.
6. [Milan][Enhancements] 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.
7. [Milan][Enhancements] Add FSRM and ERMSB items support. (Milan only, Rome not support. PI 1009 change default enable (Auto).)
8. [Milan][Enhancements] Follow the SMBIOS template sync the chassis type from FRU0 to SMBIOS Type 03, only for H12 projects.
9. [Milan][Enhancements] Enhance the solution for the error/warning message from dmidecode after a modification.
10. Update AGESA RomePI to 1.0.0.F based on 5.14_RomeCrb_0ACMK026 for AMD-SB-1032.
11. Remove "AMI Graphic Output Protocol Policy" in Advance page.
12. [Milan][Rome][Enhancements][SecurityErase] Modified GetVariable() service for buffer overflow in certain cases.

13. [Milan][Rome][Fixes] Fixed that the PCIe Link Width of AOC-SLG4-2H8M2 is downgraded to x4.
14. [Milan][Rome][Enhancements] Restore SMCI secure boot keys and Update Secure Boot DB variable. (Unknown certificate "Addtrust External CA Root" is expired on May 30th 2020)

2.5 (09/08/2022)

1. Update MilanPI to 1.0.0.9 based on 5.22_MilanCrb_0ACOU020.
2. Remove "Vendor Keys" in security page.
3. Modify String naming from SMCI to Supermicro.
4. Update DBX file to fix Secure Boot Bypass issue.
5. Update AGESA RomePI to 1.0.0.E based on 5.14_RomeCrb_0ACMK025.

2.4 (04/14/2022)

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

2.3 (10/20/2021)

1. Update BIOS revision.
2. Add Redfish/SUM Secure Boot feature, update OOB for secure boot and reserve Key.
3. Refer Whitley SVN 3116/3114 to update SmcHttpBoot module.
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 AMD EPYC 7003 with AMD 3D-V cache B2 stepping CPU microcode to patch Erratum #1381 Processor May Hang When Coherency Probe Hits Instruction Cache Line While Evicted.
9. a) BMC implemented a workaround for getting around this issue. (BMC FW need 1.01.01(SW-BMC)/1.01.07(HW1) or later version), b) Supported EUI-48 Locally Administered MAC Address. c) Degenerated the Device Type of Interface Specific Data in Redfish Host Interface DMI type 42 from USB V2 (0x04) to USB V1 (0x02)
10. Disable EFI iSCSI support for security concern.

11. Exposed Setup items "BankGroupSwapAlt", "SEV-SNP Support", "Enhanced Preferred IO Mode" and "Root Complex 0x00~0xE0 LCLK Frequency".
12. Disable "Wait For "F1" If Error".
13. BIOS didn't update AMD CBS tokens correctly

2.1 (06/02/2021)

1. Update BIOS revision.
2. Description: Update AGESA RomePI to 1.0.0.B.
3. Set all OPROM control items to Legacy when boot mode set to Dual.
4. Add Redfish/SUM Secure Boot feature, update OOB for secure boot and reserve Key.
5. Remove legacy iSCSI support of H12 BIOS.
6. Added force next boot to UEFI Shell support.
7. Update AGESA MilanPI to 1.0.0.2.
8. Update A011 GN B1 microcode 0A00111D.
9. Install U.2 NVMe device on BPN, the device cannot hot plug under windows.
10. Fixed BIOS recovery happened used AFU to clear event log and then AC cycle the system.

2.0 (02/22/2021)

1. [Rome/Next gen BIOS] Change BIOS revision to 2.0.
2. [Next gen BIOS] Update AGESA Next genPI to 1.0.0.1
3. [Next gen BIOS] Update A011 GN B1 microcode 0A001119
4. [Rome BIOS] Update AGESA RomePI to 1.0.0.A
5. [Rome/Next gen BIOS] Fix IPV6 disable in the IPMI GUI but BIOS initialize will appear IPV6 address
6. [Rome/Next gen BIOS] Per Platform Management FRU Information Storage Definition v1.1 to enhance SMBIOS Type39 System Power Supply information.
7. [Rome BIOS] Update 8310 SSP-B0 microcode 830104D.
8. [Rome BIOS] Expose Relaxed Ordering setup item.
9. [Rome BIOS] Support two different Type 41 name description for Broadcom LAN 1G/10G SKU
10. [Rome BIOS] Support preserve BIOS password feature for ROT project.
11. [Rome BIOS] Add the workaround for CPLD 18h BOOT_OK problem until CPLD fix the issue.
12. [Rome BIOS] Exposed below items for GPU performance tuning.
13. 1. TSME, 2. DDR Power Down Enable, 3. PCIe Ten Bit Support
14. Fixed "Update IPMI LAN Configuration" will keep Yes when "IPv6 support" setup item disabled.
15. Fixed SATA SGPIO LED not active issue
16. Fixed the incorrect M.2 description in SMBIOS type 9 and BIOS setup
17. [Rome BIOS] Support dynamic adjust the SATA strings for H12SSL-NT only.