

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	H12SSFF-AN6
Release Version	3.1
Release Date	Jan/20/2025
Build Date	Jan/20/2025
Previous Version	2.7
Update Category	Critical
Dependencies	BMC:01.05.32 (BMC_H12AST2600-ROT-9201MS_20250204_01.05.32_STDs)
Important Notes	BIOS image: BIOS_H12SSFF-1C19_20250120_3.1_STDsp.bin BIOS image and flash utility package: BIOS_H12SSFF-1C19_20250120_3.1_STDsp.zip Notice: 1. BIOS R2.0 and above supports 7002 and next generation processors. 2. Flash Utility in package supports BIOS R1.x update to R2.x only, cannot roll back.
Enhancements	1. [Milan][Enhancements] Update MilanPI to 1.0.0.B based on 5.22_MilanCrb_OACOU023. 2. [Rome][Enhancements] Update AGESA RomePI to 1.0.0.H based on 5.14_RomeCrb_OACMK028. 3. [Milan][Enhancements] Update Milan SEV FW version from 1.37.7 to 1.37.10 for AMD-SN-3005: AMD INV D Instruction 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_OACOU024. 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. 11. [Rome][Milan][Enhancements] Update SA50235_Supplement(Extended Image Parser Corruption Vulnerability) to address 01. BRLY-LOGOFAIL-2023-013(Score 5.1) 02. BRLY-LOGOFAIL-2023-014(Score 4.4) 03. BRLY-LOGOFAIL-2023-015(Score 4.4) 04. BRLY-LOGOFAIL-2023-016(Score 7.5) 05. BRLY-LOGOFAIL-2023-017(Score 7.5) 06. BRLY-LOGOFAIL-2023-018(Score 7.5) 07. BRLY-LOGOFAIL-2023-019(Score 7.5) 08. BRLY-LOGOFAIL-2023-020(Score 7.5) 09. BRLY-LOGOFAIL-2023-021(Score 4.1) 10. BRLY-LOGOFAIL-2023-022(Score 7.5) 11. BRLY-LOGOFAIL-2023-023(Score 7.5) 12. BRLY-LOGOFAIL-2023-024(Score 7.5) 12. [Rome][Milan][Enhancements] Update secure boot KEK and DB (Fellow EagleStream SVN 2926). 13. [Rome][Milan][Enhancements] Fix HostInterface On/Off test will drop in 4x times in UEFI Shell. 14. [Rome][Enhancements] Update AMI Modules based on 5.14_RomeCrb_OACMK029. 15. [Rome][Enhancements] Update AMI Modules based on 5.14_RomeCrb_OACMK030. 16. [Rome][Milan][Enhancements] Add AMI Resizable BAR support. 17. [Rome][Milan][Enhancements] Enable ASPM in ACPI FACP when pcie ASPM is enabled. 18. [Rome][Milan][Enhancements] Add SMC Debug log support. 19. [Milan][Enhancements] Update AMI Modules based on (BETA)5.22_MilanCrb_OACOU025. 20. [Milan][Enhancements] Add SMC_OS_PERFORMANCE_ENHANCE item 21. [Rome][Milan][Enhancements] Set Chassis type in smbios to default (0x11) when Chassis type from fru is 0x00 or 0xFF or NULL. 22. [Rome][Enhancements] Update AMI Modules based on 5.14_RomeCrb_OACMK033. 23. [Milan][Enhancements] Update AGESA MilanPI to 1.0.0.E based on 5.22_MilanCrb_OACOU028. 24. [Rome][Enhancements] Update SA50289(TianoCompress Privilege Escalation Vulnerability) to address CVE-119 25. [Rome][Enhancements] Update AMI Modules based on 5.14_RomeCrb_OACMK034. 26. [Milan][Enhancements] Update AMI Modules based on 5.22_MilanCrb_OACOU029.
--	---

New features	N/A
Fixes	1. [Milan][Rome][Fixes] Fixed memory multi-bit error will report to correctable error. 2. [Milan][Rome][Fixes] Check Update SMBIOS Type2 priority via superedit fail. 3. [Rome][Milan][Fixes] Automated PXE boot OS install issue.

Release Notes from Previous Release(s)

2.7(10/25/2023)

[Enhancements]

1. Updated MilanPI to 1.0.0.B based on 5.22_MilanCrb_0ACOU022.
2. Updated AGESA RomePI to 1.0.0.G based on 5.14_RomeCrb_0ACMK027.
3. Support for changing Pxe from Uefi(U)/Legacy(L) to L/U through Redfish.
4. Restored SMCI secure boot keys and Update Secure Boot DB variable. (Unknown certificate "Addtrust External CA Root" expired on May 30th 2020).

[Fixes]

1. Set RDIMM\LRDIMM\3DSDIMM memory throttling trip-point to 85C part II.
2. Fixed some dmivar unfit with ami sbmbios settings

2.5 (02/06/2023)

[Enhancements]

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

2.4 (04/15/2022)

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

2.3 (10/21/2021)

1. Changed BIOS revision to 2.3.
2. Added support in SUM to upload and delete HTTPS TLS certificate.
3. Set the BIOS setting "Relaxed Ordering default" to Enabled.
4. Updated AGESA MilanPI to 1.0.0.6.
5. Updated A010 GN B0 microcode 0A00104C.
6. Updated AGESA RomePI to 1.0.0.C.
7. Exposed Setup item "Enhanced Preferred IO Mode".
8. Fixed the BMC Redfish Host Interface named as ethX when CDN was disabled.
9. Disabled Legacy/EFI iSCSI support.
10. Exposed the BIOS setting "BankGroupSwapAlt", "SEV-SNP Support", "Enhanced Preferred IO Mode" and "Root Complex 0x00~0xE0 LCLK Frequency".
11. Changed the default of "Wait For "F1" If Error" to Disabled.
12. Set all oprom control items to Legacy when boot mode set to Dual.
13. Added Redfish/SUM Secure Boot feature and updated OOB for secure boot and reserve.
14. Added "Force Next Boot" to UEFI shell support.
15. Updated A011 GN B1 microcode 0A00111D.
16. Fixed Intel X550 dropped during an on-off aging.
17. Fixed SUM cannot modify AMD CBS settings.

2.1 (06/04/2021)

1. Changed BIOS revision to 2.1.
2. Updated AGESA RomePI to 1.0.0.B.
3. Set all OPRM control items to Legacy when boot mode set to Dual.
4. Added force next boot to UEFI Shell support.
5. Updated AGESA MilanPI to 1.0.0.2.
6. Updated A011 GN B1 microcode 0A00111D.
7. Fixed problem of an AIOM card (Intel X550) dropping during an on/off aging.

2.0a (04/22/2021)

1. Changed BIOS revision to 2.0a.
2. Fixed problem of AFU/clnevnlog causing ROT BIOS recovery.

2.0 (02/23/2021)

1. Changed BIOS revision to 2.0.
2. Added support for both AMD EPYC 7002 and next generation processors.
3. Updated A011 GN B1 microcode 0A001119.
4. Updated AGESA RomePI to 1.0.0.A.
5. Fixed problem of BIOS initialization showing IPV6 address when IPV6 is disabled in the IPMI GUI.
6. Enhanced SMBIOS Type39 System Power Supply information.

1.0b (2021/01/28)

1. Reaction to BMC 00.01.25, BMC remove the reset from a changing LAN data within the 30/20 command. BIOS remove the patch.

1.0a (2020/12/19)

1. Changed BIOS revision to 1.0a

2. Patched problem of POST randomly hanging at B2 during AC aging.
3. Corrected OEM FID VBIOS version.

1.0 (2020/12/14)

Initial release.