

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	H12SSG-ANP6
Release Version	2.9
Release Date	5/3/2024
Build Date	5/3/2024
Previous Version	2.4
Update Category	Recommended
Dependencies	IPMI firmware R 00.01.15
Important Notes	BIOS Image: BIOS_H12SSG-ANP6-1C2C_20240503_2.9_STDsp.bin BIOS Update Package: BIOS_H12SSG-ANP6-1C2C_20240503_2.9_STDsp.zip
Enhancements	1. Updated 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) 2. Updated secure boot KEK and DB (Fellow EagleStream SVN 2926). 3. Fixed HostInterface On/Off test that drops in 4x times in UEFI Shell. 4. Updated AMI Modules based on 5.14_RomeCrb_0ACMK029. 5. Updated AMI Modules based on 5.14_RomeCrb_0ACMK030. 6. Added AMI Resizable BAR support. 7. Enabled ASPM in ACPI FACP when pcie ASPM is enabled. 8. Added SMC Debug log support. 9. Updated AMI Modules based on (BETA)5.22_MilanCrb_0ACOU025. 10. Added SMC_OS_PERFORMANCE_ENHANCE item 11. Updated AGESA MilanPI to 1.0.0.C based on 5.22_MilanCrb_0ACOU024. 12. Updated AGESA RomePI to 1.0.0.H based on 5.14_RomeCrb_0ACMK028. 13. Updated Milan SEV FW version from 1.37.7 to 1.37.10 for AMD-SN-3005: AMD INVD Instruction Security Notice.

	14. Updated SA50216_Supplement(LogoFAIL Vulnerability). 15. Fixed MP1(SMU) and CPU WDT uncorrectable error no event log issue. 16. Disabled "Correctable/Non-Fatal error reporting enable" bits when BIOS item "PCI AER support" set Disabled. 17. Updated SA50218_Supplement(Vulnerabilities in EDK2 NetworkPkg). 18. Updated SA50230_Supplement(Image Parser Corruption Vulnerability). 19. Disabled ASPM in ACPI FACP when pcie ASPM is disabled. 20. Added support for changing Pxe from Uefi(U)/Legacy(L) to L/U through Redfish. 21. Updated 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. 22. Added support for Supermicro System LockDown feature. 23. Updated Rome B0 stepping CPU microcode 0x0830107A for AMD-SB-7008 Security Bulletin to address CVE-2023-20593 issue. 24. Added Rocky Linux Boot Option Name. 25. 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. 26. Added FSRM and ERMSB items support. (Milan only, Rome not support. PI 1009 change default enable (Auto).) 27. Followed the SMBIOS template to sync the chassis type from FRU0 to SMBIOS Type 03, only for H12 projects. 28. Added enhancement to the solution for the error/warning message from dmidecode after a modification. 29. Removed "AMI Graphic Output Protocol Policy" in Advance page. 30. [SecurityErase] Modified GetVariable() service for buffer overflow in certain cases.
New features	N/A
Fixes	1. Automated PXE boot OS install issue. 2. Fixed memory multi-bit error will report to correctable error. 3. Checked Update SMBIOS Type2 priority via superedit fail. 4. Set RDIMM\LRDIMM\3DSDIMM memory throttling trip-point @85C part II. 5. Fixed some dmivar that are unfit with ami smbios settings. 6. Fixed BMC web can't show LAN MAC address correctly with X710.

Release Notes from Previous Release(s)

2.4 (3/16/2022)

1. First release TRP Pro combined BIOS image.

1.0 (12/30/2021)

Initial Release