

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-AN6
Release Version	3.3
Release Date	3/28/2025
Build Date	3/28/2025
Previous Version	3.0
Update Category	Recommended
Dependencies	IPMI firmware R 00.01.20
Important Notes	BIOS Image: BIOS_H12SSG-1C2C_20250328_3.3_STDsp.bin BIOS Update Package: BIOS_H12SSG-1C2C_20250328_3.3_STDsp.zip
Enhancements	1. Updated AMI modules based on 5.14_RomeCrb_0ACMK033. 2. Updated AGESA MilanPI to 1.0.0.E based on 5.22_MilanCrb_0ACOU028. 3. Updated SA50289 (TianoCompress Privilege Escalation Vulnerability) to address CVE-119. 4. Updated AMI modules based on 5.14_RomeCrb_0ACMK034. 5. Updated AMI modules based on 5.22_MilanCrb_0ACOU029. 6. Updated AMI modules based on 5.14_RomeCrb_0ACMK035. 7. Updated Legacy Serial Redirection module from MAINT_LegacySreDir_13.01 to MAINT_LegacySreDir_14.01. 8. Updated AMI modules based on 5.22_MilanCrb_0ACOU030. 9. Updated Secure Boot DBX to address AMI SA50300 (CVE-2024-7344\CVE-2023-24932 (8.2 High/6.7 Middle)) security issue.
New features	N/A
Fixes	N/A

Release Notes from Previous Release(s)

3.0 (7/29/2024)

1. Filled DUID with UUID in all systems to avoid DUID in IPv6 DHCP being the same.
2. Updated AMI Modules based on 5.14_RomeCrb_OACMK031.
3. Updated AMI Modules based on 5.14_RomeCrb_OACMK032.
4. For UsbBus.c, added USB IAD device class/subclass/protocol support for ECM RNDIS.
5. Updated AGESA MilanPI to 1.0.0.D based on 5.22_MilanCrb_OACOU027.

2.9 (5/29/2024)

1. 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.
2. Added support for Supermicro System LockDown feature.
3. Updated Rome B0 stepping CPU microcode 0x0830107A for AMD-SB-7008 Security Bulletin to address CVE-2023-20593 issue.
4. Added Rocky Linux Boot Option Name.
5. Updated AGESA MilanPI to 1.0.0.C based on 5.22_MilanCrb_OACOU024.
6. Updated AGESA RomePI to 1.0.0.H based on 5.14_RomeCrb_OACMK028.
7. Added support for changing Pxe from Uefi(U)/Legacy(L) to L/U through Redfish.
8. 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)
9. Updated secure boot KEK and DB.
10. Fixed HostInterface On/Off test will drop in 4x times in UEFI Shell.
11. Updated AMI Modules based on 5.14_RomeCrb_OACMK029.
12. Updated AMI Modules based on 5.14_RomeCrb_OACMK030.
13. Added AMI Resizable BAR support.
14. Enabled ASPM in ACPI FACP when pcie ASPM is enabled.
15. Added SMC Debug log support.
16. Updated AMI Modules based on 5.22_MilanCrb_OACOU025.
17. Added SMC_OS_PERFORMANCE_ENHANCE item
18. Updated Milan SEV FW version from 1.37.7 to 1.37.10 for AMD-SN-3005: AMD INVD Instruction Security Notice.
19. Updated SA50216_Supplement (LogoFAIL Vulnerability).
20. Fixed MP1(SMU) and CPU WDT uncorrectable error no event log issue.
21. Disabled "Correctable/Non-Fatal error reporting enable" bits when BIOS item "PCI AER support" set Disabled.
22. Updated SA50218_Supplement (Vulnerabilities in EDK2 NetworkPkg).
23. Updated SA50230_Supplement (Image Parser Corruption Vulnerability).
24. Disabled ASPM in ACPI FACP when pcie ASPM is disabled.

25. Set Chassis type in smbios to default (0x11) when Chassis type from fru is 0x00 or 0xFF or NULL.
26. Fixed BMC web can't show LAN MAC address correctly with X710.
27. Fixed that the PCIe Link Width of AOC-SLG4-2H8M2 is downgraded to x4.
28. Set RDIMM\LRDIMM\3DSDIMM memory throttling trip-point @85C part II.
29. Fixed some dmivar unfit with ami smbios settings.
30. Automated PXE boot OS install issue.
31. Fixed the problem that the AMD Radon PRO W7500 & W7600 VGA card cannot be displayed in the shell or BIOS setup menu.
32. Fixed memory multi-bit error will report to correctable error.
33. Fixed check Update SMBIOS Type2 priority via superedit failure.

2.4 (6/23/2022)

1. Changed BIOS revision to 2.4.
2. Added setup item, "ASPM Support" in PCIe/PCI/PnP Configuration Page.
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 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. Added setup item, "SNP Memory (RMP Table) Coverage" and "Amount of Memory to Cover" in CPU Configuration Page.
9. Implemented work around solution for AOC-ATGC-i2TM PCIe gen drop problem on H12SSG-AN6.

2.3 (10/22/2021)

1. Changed BIOS revision to 2.3.
2. Updated AGESA RomePI to 1.0.0.C.
3. Exposed Setup item "Enhanced Preferred IO Mode".
4. Updated AGESA MilanPI to 1.0.0.6.
5. Patched case of BMC Redfish Host Interface being named ethX when CDN is disabled under Linux OS.
6. Disabled EFI iSCSI support.
7. Exposed Setup items "BankGroupSwapAlt", "SEV-SNP Support", "Enhanced Preferred IO Mode", and "Root Complex 0x00~0xE0 LCLK Frequency".
8. Changed default of "Wait For "F1" If Error" to Disable.
9. Updated B0 Milan microcode 0x0A00104C, B1 Milan microcode 0x0A001143, and B2 Milan-X microcode 0x0A001223 to patch Erratum #1381 problem of processor hanging when coherency probe hits instruction cache line while evicted.

2.2 (7/31/2021)

1. Changed BIOS revision to 2.2.
2. Set all OPROM control items to Legacy when boot mode is set to Dual.
3. Added Redfish/SUM Secure Boot feature and updated OOB for secure boot and reserve key.
4. Removed legacy iSCSI support of H12 BIOS.
5. Added force next boot to UEFI Shell support.

6. Added support for SUM upload/deletion of HTTPS TLS certificate (default enabled by TOKEN "Sum_UploadTlsKey_SUPPORT").
7. Set Relaxed Ordering default to Enabled.
8. Updated AGESA MilanPI to 1.0.0.4.
9. Updated A010 GN B0 microcode 0A001046, A011 GN B1 microcode 0A001137, and A012 GN B2 microcode 0A00121D.
10. Updated AGESA RomePI to 1.0.0.C.
11. Fixed inability of SUM to modify AMD CBS settings.
12. Fixed missing sensor information on IPMI WebGUI.

2.0 (5/05/2021)

Initial Release