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	**H13SST-G/GC**
Release Version	**3.4**
Release Date	**05/05/2025**
Previous Version	**3.1**
Update Category	**Recommend**
Dependencies	**N/A**
Important Notes	**For AMD EPYC™ 9005 Series Processor support, please ensure your motherboard revision is R2.0 or higher. The BIOS and BMC package versions should be BIOS V3.0 or higher and BMC V01.03.03 or higher.** **Please note that if you would like to roll back the BIOS from V3.x (AMD EPYC™ 9004/9005 Series Processor) dual BIOS to V1.x (AMD EPYC™ 9004 Series Processor) single BIOS, make sure to install AMD EPYC™ 9004 Series Processor before updating the BIOS.** **To support AMD EPYC™ Bergamo/Genoa-X processor, please update to BIOS v1.4 or higher.**
Enhancements	***1. [Genoa][Turin][Enhancements] Update SA50292 (OpenSSL 3.1.4 Vulnerabilities Fixes) to address CVE-2023-6237(Medium, 5.9), CVE-2024-5535(High, 9.1), CVE-2024-6119(High, 7.5) security issue.*** ***2. [Genoa] Update to 5.27_GenoaCrb_0ACQT028 for AGESA 1.0.0.F*** ***3. [Genoa][Turin] Update Secure Boot DBX to address AMI SA50300 (CVE-2024-7344\CVE-2023-24932 (8.2 High/6.7 Middle)) security issue*** ***4. [Turin] Disable support automatically change memory speed.*** ***5. Update BIOS version to 3.4 ; For Dual-image support BIOS revision.*** ***6. Remove Supermicro product CA 2018 key from DB;Supermicro product CA 2018 key format is not supported from Linux kernel 5.0 or later.*** ***7. [Turin] Update AGESA 1.0.0.5.***

	8. [Genoa]Update Genoa SEV FW version from 1.37.2A to 1.37.2B for potential security issue; For CVE-2023-20585, CVE-2024-21953.
New features	***N/A***
Fixes	***1. [Genoa][Fixes] Disable LongSerialNumber support.*** ***2. [Genoa][Fixes] Fix Quiet Boot can't be loaded to default after clear cmos.***

3.1 (12/26/2024)

1. *[Enhancements] Update to 5.27_GenoaCrb_0ACQT027 for AGESA 1.0.0.E*
2. *[Enhancements] Update to 5.35_TurinCrb_0ACST017 for AGESA 1.0.0.3*
3. *[Enhancements][SmcSecureBoot] Exposed "Secure Boot Mode" setup item to SAA.*
4. *[Enhancements] Implement inject OA3 Key function.*
5. *[Fixes] Fix BMC IPV6 setup items don't work*
6. *[Fixes]BIOS cannot restart the system through IO CF9 0xE after clearing CMOS through BMC IPMI and executing power reset.*
7. *[Fixes] Fix Rocky OS RAID 1 can't boot.*

3.0 (10/04/2024)

1. *Update to 5.27_GenoaCrb_0ACQT025 for AGESA 1.0.0.C*
2. *Update SA50218 (Vulnerability in EDK2 NetworkPkg/PixieFail VU#132380) to address CVE-2023-45229/CWE-125 (Medium, 6.5), CVE-2023-45230/CWE-119 (High, 8.3), CVE-2023-45231/CWE-125 (Medium, 6.5), CVE-2023-45232/CWE-835 (Medium, 6.5), CVE-2023-45233/CWE-835 (Medium, 6.5), CVE-2023-45234/CWE-119 (High, 8.3), CVE-2023-45235/CWE-119 (High, 8.3)*
3. *Update AMITSE module for AMI SA50216 and SA50230 Security Advisories(LogoFAIL Vulnerability) to address CVE-2023-39538(7.5, High) and CVE-2023-39539(7.5, High) security issues*
4. *Update SA50235 (Extended Image Parser Corruption Correction) to address BRLY-LOGOFAIL-2023-013(Medium, 5.1), BRLY-LOGOFAIL-2023-014(Medium, 4.4), BRLY-LOGOFAIL-2023-015(Medium, 4.4), BRLY-LOGOFAIL-2023-016(High, 7.5), BRLY-LOGOFAIL-2023-017(High, 7.5), BRLY-LOGOFAIL-2023-018(High, 7.5), BRLY-LOGOFAIL-2023-019(High, 7.5), BRLY-LOGOFAIL-2023-020(High, 7.5), BRLY-LOGOFAIL-2023-021(Medium, 4.1), BRLY-LOGOFAIL-2023-022(High, 7.5), BRLY-LOGOFAIL-2023-023(High, 7.5), BRLY-LOGOFAIL-2023-024(High, 7.5)*
5. *Update secure boot KEK/DB to add new Microsoft certificate.*
6. *Disable ASPM in ACPI FACP when pcie ASPM is disabled.*
7. *Follow SW-PM's command change BIOS default setting for enable AMD ADDC by default.*
8. *Report GPU information to type 40 if card is a GPU hybrid card. (GPU system only)*
9. *Remove lan condition when get VPD data.*
10. *Update SEL support for Post Package Repair and MBIST.*
11. *Fix "CCD control" and "Core Control" items can't work.*

12. Add FBO group in BIOS cfg file dump from SUM.
13. Fix CPU freq. is incorrect in setup.
14. Fixed change boot order by IPMI function abnormal issue.
15. Fixed ACPI BIOS error(CSMI) in dmesg.

1.9 (05/28/2024)

1. Update to 5.27_GenoaCrb_0ACQT025 for AGESA 1.0.0.C
2. Update SA50218 (Vulnerability in EDK2 NetworkPkg/PixieFail VU#132380) to address CVE-2023-45229/CWE-125 (Medium, 6.5), CVE-2023-45230/CWE-119 (High, 8.3), CVE-2023-45231/CWE-125 (Medium, 6.5), CVE-2023-45232/CWE-835 (Medium, 6.5), CVE-2023-45233/CWE-835 (Medium, 6.5), CVE-2023-45234/CWE-119 (High, 8.3), CVE-2023-45235/CWE-119 (High, 8.3)
3. Update AMITSE module for AMI SA50216 and SA50230 Security Advisories(LogoFAIL Vulnerability) to address CVE-2023-39538(7.5, High) and CVE-2023-39539(7.5, High) security issues
4. Update SA50235 (Extended Image Parser Corruption Correction) to address BRLY-LOGOFAIL-2023-013(Medium, 5.1), BRLY-LOGOFAIL-2023-014(Medium, 4.4), BRLY-LOGOFAIL-2023-015(Medium, 4.4), BRLY-LOGOFAIL-2023-016(High, 7.5), BRLY-LOGOFAIL-2023-017(High, 7.5), BRLY-LOGOFAIL-2023-018(High, 7.5), BRLY-LOGOFAIL-2023-019(High, 7.5), BRLY-LOGOFAIL-2023-020(High, 7.5), BRLY-LOGOFAIL-2023-021(Medium, 4.1), BRLY-LOGOFAIL-2023-022(High, 7.5), BRLY-LOGOFAIL-2023-023(High, 7.5), BRLY-LOGOFAIL-2023-024(High, 7.5)
5. Update secure boot KEK/DB to add new Microsoft certificate.
6. Disable ASPM in ACPI FACP when pcie ASPM is disabled.
7. Follow SW-PM's command change BIOS default setting for enable AMD ADDC by default.
8. Report GPU information to type 40 if card is a GPU hybrid card. (GPU system only)
9. Remove lan condition when get VPD data.
10. Update SEL support for Post Package Repair and MBIST.
11. Fix "CCD control" and "Core Control" items can't work.
12. Add FBO group in BIOS cfg file dump from SUM.
13. Fix CPU freq. is incorrect in setup.
14. Fixed change boot order by IPMI function abnormal issue.
15. Fixed ACPI BIOS error(CSMI) in dmesg.

1.6 (11/30/2023)

1. Update to 5.27_GenoaCrb_0ACQT022 for AGESA 1.0.0.9 with patch
2. Update SecureBoot and AmiSecureBootPkg to correct secure boot system mode.
3. Fixed Memory Pmic event log DIMM location incorrect.
4. Fix duplicate lan string in boot order
5. Fixed an issue that "Present but not trained" is displayed in the memory information when no DIMM was installed.
6. Patch M.2 slot 2 sometimes drop.

7. *Correct NVMe sequence in Rear IO sku.*

1.5a (08/14/2023)

1. *Updated AMI label to 5.27_GenoaCrb_0ACQT020 for AGESA 1.0.0.7 with patch*
2. *Change Memory information unit to MT/s*
3. *Enhance the solution for the error/warning message from dmidecode after a modification by AMIDE.*
4. *Trigger Memory Enhanced PPR + SuperDiag after changing boot option to "Diag" via BMC*
5. *Hide "Local APIC Mode"*
6. *Update Pcode for erratum#1484/1485*
7. *Fix BMC VLAN status show incorrectly*
8. *Add workaround for HII can't be parsed from BIOS ROM*
9. *Fix AMIBCP can't change CPU settings*
10. *Fix boot order can't be preserved after updating BIOS*
11. *Fix IOMMU can'be be kept after updating BIOS*
12. *Fix SMT control can'be be kept after updating BIOS*

1.4** **(03/22/2023**)***

1. *Updated AMI label to 5.27_GenoaCrb_0ACQT018 for AGESA 1.0.0.6*
2. *Fixed MCA correctable error cannot trigger when MCEON disabled.*
3. *Fix DDR5 speed not shown when "Quiet Boot" = Disable.*
4. *Fix BMC VLAN status show incorrectly.*

1.1 (01/17/2023)

1. *Updated AMI label to 5.27_GenoaCrb_0ACQT016 for AGESA 1.0.0.3*
2. *Add patch for MICRON NVMe lane drop*

1.0 (10/28/2022)

1. *First release*