

BIOS Release Notes

TITLE

SUBJECT: MS33-AR0 BIOS Release Notes version [R11](#)

System: [MS33-AR0-000](#)

About This Release

Build Date: [2025/02/22](#)

BIOS Checksum: [0xA46C7DBE](#) (16M), [0x8C735447](#) (64M)

Release Owner: kimberly.lin

BIOS Components/Contents

Processor stepping(s) supported: Intel® Sapphire Rapids-SP/Emerald Rapids-SP processor

System hardware configurations supported: MS33-AR0

Microcode updates versions:

| CPUID | Family | Microcode Update ID |
|-------|--|---------------------|
| 806f3 | Sapphire Rapids Production D-0 | 0d0004b1 |
| 806f8 | Sapphire Rapids All HBM Production B | 2c0003e0 |
| 806f8 | Sapphire Rapids All Production XCC E / MCC S / EE LCC U | 2b000620 |
| c06f2 | Processor Emerald Rapids Production XCC A1 / MCC R1 | 21000291 |

IPMI support:

AMI Kernel version: [Gbt_Kernel_107_47](#)

Intel CSI/MRC Package version: [113.D55](#)

SPI Descriptor version: [06.01.04.075.0](#)

OPROM version :

BIOS Release Notes

| OPROM | Version |
|-----------------------|-----------------|
| INTEL 10G LAN EFI | 7.0.19 |
| INTEL 10G PXE | 2.3.24 |
| AST2600 VGA | 1.13.03 |
| INTEL RAID PACKAGE | RSTe 8.6.0.1136 |

Installation Notes

IMPORTANT NOTES:

1. Please extract the MS33-AR0_R11.zip to a bootable diskette that use FAT/FAT32 format

BIOS UPDATE INSTRUCTIONS FOR EFI Shell:

1. Insert USB flash drive to system for BIOS upgrade.
2. Power on system and boot to Build-In Shell.
3. Enter your USB filesystem, like "fs0:" or "fsx:", "x" is your USB filesystem number
4. Execute F.nsh for bios update
5. After bios flash finish, system must Power-Off to have the changes take effect.

BIOS UPDATE INSTRUCTIONS FOR Windows:

1. Insert bios update USB flash drive.
2. Use Command Shell.
3. Enter \Tool\Win32 and execute f.bat for Windows 32bit.
Or
Enter \Tool\Win64 and execute f.bat for Windows 64bit.
4. After bios flash finish, system must Power-Off to have the changes take effect.

BIOS UPDATE FOR Easy BIOS Refresh:

1. The system supports remotely update BIOS if BMC existent.
2. Please download the Easy BIOS Refresh User Guide from Gigabyte website, target system support page.

BIOS Version CHECK INSTRUCTIONS:

1. Power on system and press during POST
2. The bios version shows on the first main page

Known Issues/Workarounds

BIOS Release Notes

Issues fixed in this version

R11

1. [Feature] Fine tune BIOS setup item default.
 2. [Feature] Improve KCS protocol.
 3. [Feature] Support Microsoft Option ROM UEFI CA 2023 for Secure Boot.
-

R10

1. [Feature] Fine-tune Redfish display content.
-

R09

1. [Feature] Update RC 113.D55 (EagleStream uPLR3 BKC 2024 WW37).
 2. [Feature] Update EMR Microcode : EMR Production A* / R* Step:
m_87_c06f2_21000291.pdb;
 3. [Feature] Update SPR Microcode : SPR Production E* / S* Step:
m_87_806f8_2b000620.pdb;SPR HBM Production B* Step: m_10_806f8_2c0003e0.pdb;
 4. [Feature] Include INTEL-SA-01139 for CVE-2024-31157/CVE-2024-28047/CVE-2024-39279.
 5. [Feature] Include INTEL-SA-01166 for CVE-2024-31068.
 6. [Feature] Include INTEL-SA-01194 for CVE-2024-37020.
 7. [Feature] Include INTEL-SA-01120 for CVE-2024-25571.
 8. [Feature] Include INTEL-SA-01198 for CVE-2024-21859/CVE-2024-31155.
 9. [Feature] Include INTEL-SA-01152 for CVE-2024-26021/CVE-2024-30211.
 10. [Feature] Include INTEL-SA-01196 for CVE-2024-36242.
 11. [Feature] Include INTEL-SA-01192 for CVE-2024-33607.
-

R08

1. [Feature] Update RC 111.D23 (EagleStream uPLR2 BKC 2024 WW30).
2. [Feature] Update EMR Microcode : EMR Production A* / R* Step:
m_87_c06f2_21000283.pdb;
3. [Feature] Update SPR Microcode : SPR Production E* / S* Step:
m_87_806f8_2b000603.pdb;SPR HBM Production B* Step: m_10_806f8_2c0003d3.pdb;
4. [Feature] Update UEFI VROC to VROC v8.6.0.1136.
5. [Feature] Update TDX Module to TDX_1.5.06.00.744
6. [Bug Fix] Include INTEL-SA-01097 for CVE-2024-24968
7. [Bug Fix] Include INTEL-SA-01103 for CVE-2024-23984.
8. [Bug Fix] Include INTEL-SA-01079 for CVE-2024-21820/CVE-2024-23918.
9. [Bug Fix] Include INTEL-SA-01071 for CVE-2024-21829/CVE-2024-21781/CVE-2024-23599.
10. [Bug Fix] Include INTEL-SA-01085 for CVE-2024-25565.
11. [Bug Fix] Include INTEL-SA-01101 for CVE-2024-21853.

BIOS Release Notes

12. [Bug Fix] Include INTEL-SA-01099 for CVE-2024-27457.
 13. [Bug Fix] Include INTEL-SA-01111 for CVE-2024-22185/CVE-2024-24985.
 14. [Bug Fix] Include INTEL-SA-01076 for CVE-2024-21850.
 15. [Bug Fix] Include AMI SA50158 for CWE-269.
-

R07

1. [Feature] Update RC 109.D34 (EagleStream uPLR1 OOB BKC 2024).
 2. [Feature] Update EMR Microcode : EMR Production A1/R1-Stepping:m_87_c06f2_21000240.pdb;
 3. [Feature] Update SPR Microcode : SPR Production E-Stepping:m_87_806f8_2b0005d1.pdb;SPR HBM Production B-Stepping:m_10_806f8_2c0003a1.pdb;
 4. [Feature] Fine tune BMC LAN IPv6 configuration page.
-

R06

1. [Feature] Fine tune Intel TDX related item.
 2. [Feature] Fine tune BMC IPv6 and IPv4 Network.
 3. [Feature] Include AMI SA50248 solution for CWE-119.
-

R05

1. [Feature] Update RC 109.D34 (EagleStream uPLR1 BKC 2024 WW12).
 2. [Feature] Update EMR Microcode : EMR Production A1/R1-Stepping:m_87_c06f2_21000230.pdb;
 3. [Feature] Update SPR Microcode : SPR Production E-Stepping:m_87_806f8_2b0005c0.pdb;SPR HBM Production B-Stepping:m_10_806f8_2c000390.pdb;
 4. [Feature] Update SPS FW to SPS_E5_06.01.04.047.0.
 5. [Feature] Update BIOS ACM / SINT to v1.1.A.
 6. [Feature] Update TDX Module to TDX_1.5.05.46.698.
 7. [Feature] Include INTEL-TA-01036 for CVE-2023-45745/CVE-2023-47855.
 8. [Feature] Include AMI SA50232 for CVE-2023-45236/CVE-2023-45237.
-

R04

1. [Bug Fix] Fix install CMT4032 can't downgrade to Gen3.
-

R03

1. [Feature] Update RC 1752.P05 (EagleStream UMR1 BKC 2024 WW05).
2. [Feature] Update EMR Microcode : No update.
3. [Feature] Update SPR Microcode : SPR Production E-Stepping:m_87_806f8_2b000590.pdb;SPR HBM Production B-

BIOS Release Notes

Stepping:m_10_806f8_2c000360.pdb;

4. [Feature] Add AMI SA50218 for below CVE :

CVE-2023-45229

CVE-2023-45230

CVE-2023-45231

CVE-2023-45232

CVE-2023-45233

CVE-2023-45234

CVE-2023-45235

5. [Feature] Add AMI SA50229 for CVE-2023-3817 and CVE-2023-2650.

6. [Feature] Add AMI SA50236 for CVE-2023-5678.

R02

1. [Feature] Update RC 107.D52 (EagleStream PV BKC 2023 WW49).

2. [Feature] Update EMR Microcode : EMR A0-Stepping: m_87_c06f2_a1000200.pdb ; EMR Production A0-Stepping:Stepping:m_87_c06f2_21000200.pdb;

3. [Feature] Add AMI SA50216 solution for CVE-2023-39539 and CVE-2023-39538.

R01

1. [Feature] Update RC 107.D20 (EagleStream BKC 2023 WW45).

2. [Feature] Update EMR Microcode : EMR A0-Stepping: m_87_c06f2_a10001d1.pdb .pdb ; EMR Production A0-Stepping:m_87_c06f2_210001B0.pdb; SPR Production E-Stepping:m_87_806f8_2b000571.pdb;SPR HBM Production B-Stepping:m_87_806f8_2c000351.pdb;

3. [Feature] Update SPS to SPS_E5_06.01.04.005.0.

4. [Feature] Update RSTe VROC driver to v8.5.0.1096.

T07

1. [Feature] Update RC 105.D74 (EagleStream BKC 2023 WW41).

2. [Feature] Update EMR Microcode : EMR A0-Stepping: m_87_c06f2_a1000190.pdb ; EMR Production A0-Stepping:m_87_c06f2_21000190.pdb; SPR Production E-Stepping:m_87_806f8_2b000541.pdb;SPR HBM Production B-Stepping:m_87_806f8_2c000321.pdb;

3. [Feature] Update SPS to SPS_E5_06.01.04.003.0.

4. [Feature] Update AST2600 vga/dp driver to 1.13.03 version.

T06

1. [Feature] Base on 2023 WW37 BKC release PC version BIOS.

T05

BIOS Release Notes

1. [Feature] Update RC 105.D74 (EagleStream BKC 2023 WW37).
 2. [Feature] Update EMR Microcode : EMR A0-Stepping: m_87_c06f2_a1000161.pdb ; EMR Production A0-Stepping:m_87_c06f2_21000161.pdb;
-

T04

1. [Feature] Update RC 105.D48 (EagleStream BKC 2023 WW35).
 2. [Feature] Update EMR Microcode : EMR A0-Stepping: m_87_c06f2_a1000160.pdb ; EMR Production A0-Stepping:m_87_c06f2_21000160.pdb;
 3. [Feature] Update VROC driver to v8.5.0.1074
-

T03

1. [Feature] Update RC 105.D20 (EagleStream BKC 2023 WW33).
 2. [Feature] Update EMR Microcode : EMR A0-Stepping: m_87_c06f2_a1000150.pdb ; EMR Production A0-Stepping:m_87_c06f2_21000140.pdb;
 3. [Feature] Update EMR Microcode : EMR A0-Stepping: m_87_c06f2_a1000150.pdb ; EMR Production A0-Stepping:m_87_c06f2_21000140.pdb;
-

T02

1. [Feature] Update RC 103.D70 (EagleStream BKC 2023 WW27).
 2. [Feature] Update EMR Microcode : EMR A0-Stepping: m_87_c06f2_a1000100.pdb ; EMR Production A0-Stepping:m_87_c06f2_210000e0.pdb;
 3. [Feature] Update EMR SPS version to SPS_E5_06.01.02.048.0.
 4. [Feature] Update VROC driver to v8.5.0.1042.
-

T01

1. [Feature] Update RC 102.D37 (EagleStream BKC 2023 WW21).
 2. [Feature] Update EMR Microcode : EMR A0-Stepping: EMR A0-Stepping: m_87_c06f2_a10000a0.pdb ; EMR Production A0-Stepping:m_87_c06f1_21000070.pdb;
 3. [Feature] Update EMR SPS version to SPS_E5_06.01.02.009.0.
 4. [Feature] Update VROC driver to v8.5.0.1020.
-