

# BIOS Release Notes

## TITLE

**SUBJECT:** MZ01-CE0 BIOS Release Notes version R40  
**System:** MZ01-CE0-00, MZ01-CE0-ES-Techdata-001, R151-Z00-ES-Techdata-001, S451-001-00, S451-001-M7, MZ01-CE1-00, MZ01-CE1-N0, R271-Z00-00, W291-Z00-00, G431-MM1-GO

### About This Release

**Build Date:** 2024/10/11  
**BIOS Checksum:** 0xCBC7A44A (16M)  
**Release Owner:** Yuan.Chen

### BIOS Components/Contents

**Processor stepping(s) supported:** AMD Rome processors  
**System hardware configurations supported:** MZ01-CE0, MZ01-CE1, MZ01-CE2  
**Microcode updates versions:**

**IPMI support:**

**AGESA PI version:** RomePI 1.0.0.K

**OPROM version :**

OPROM	Version
AST2500 VGA	1.10

### Installation Notes

#### IMPORTANT NOTES:

- Please extract the zip file 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.

## BIOS Release Notes

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 <DEL> during POST
2. The bios version shows on the first main page

### BIOS UPDATE INSTRUCTIONS FOR Web UI:

1. Connect BMC\_IP by Internet browser.
2. Click Web-UI sub-page button "Update".
3. Select Firmware Type to ROM.
4. Use Command Shell.
5. cd to /RBU.
6. Select File Path to image.RBU.
7. Click Upload.

### BIOS UPDATE INSTRUCTIONS FOR GbtUtility:

1. Please copy the BIOS\_ZIP file to GbtUtility folder.
2. Use Command Shell.
3. cd to GbtUtility folder.
4. Execute "java -jar GbtUtility.jar -H BMC\_IP update bios BIOS\_ZIP 1".

## Known Issues/Workarounds

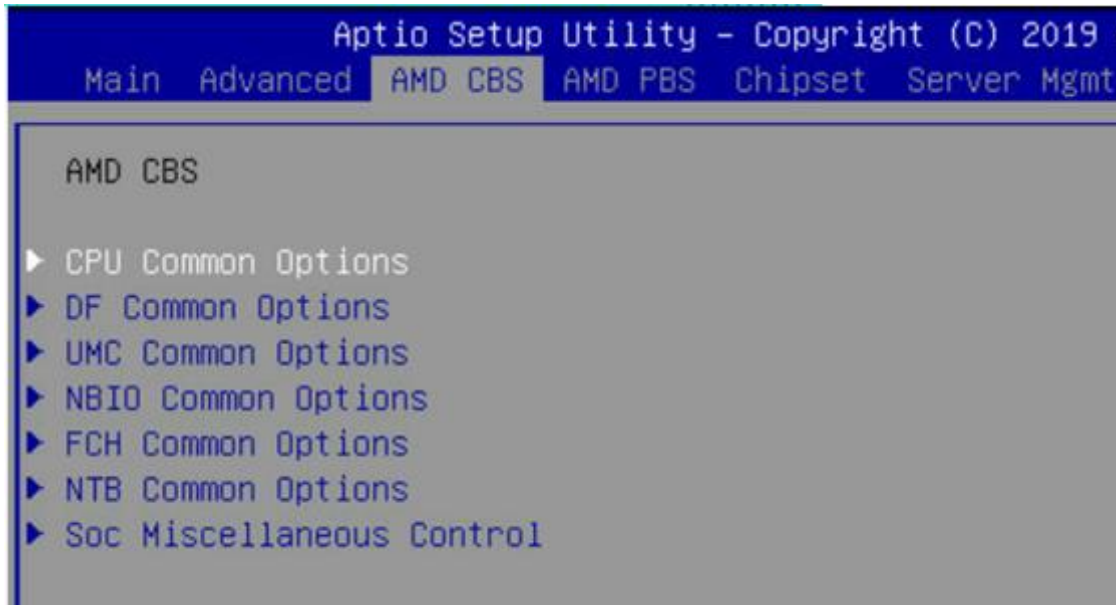
1. Windows 2016 need install KB4022723 first, then enable BIOS setup item "IOMMU"  
Nvidia VGA CUDA not support IOMMU on Linux.
2. Windows OS does not support 256 or more logical. ( Need apply below update )  
2-1 . Windows 2019 can update KB4512534 to support 256 core SMT mode.  
2-2 . Set BIOS setup item "SMT Mode" to "Auto"
3. If your side use 64 core CPU x2.  
3-1. Linux kernel need 4.19 or later version and apply AMD X2APIC patch.  
( AMD X2APIC patch Implement OS version by OS vendor define )  
3-2. Windows 2019 need install KB4512534 for Support SMT.

### PS.

BIOS setup item "SMT Mode" meant ( Simultaneous Multi-Threading ) Technology.

BIOS setup item "SMT Mode" Location as below :

## BIOS Release Notes



AMD CBS ( on BIOS Setup page bar)

▶ CPU Common Options

▶ Performance

▶ CCD/Core/Thread Enablement

▶ Accept

SMT Control: **Disable** (Default) / Auto

### Issues fixed in this version

R40 (2024/10/11)

1. [Feature] Update AGESA 1.0.0.K
2. [Feature] SMM Lock Bypass CVE-2023-31315.
3. [Bug Fix] Fix PKfail issue.
4. [Bug Fix] Fix SMBIOS Type39 PSU detected issue.

R38 (2021/11/26)

1. Update AGESA version to 1.0.0.C
2. Add check old BMC 12.44.06

R36 (2021/11/05)

1. Hide XGMI item for prevent user adjust incorrect speed.
2. Adjust CPU SATA redriver settings for G431-MM1.

R34 (2021/04/22)

1. Synchronize BIOS settings to BMC while doing remote setup on Power Policy Quick Settings.
2. Fix booting virtual image fail issue with disabled USB Device boot option in Legacy mode.
3. Send ASM Information to BMC for G431-MM1-GO.

## BIOS Release Notes

4. Adjust some GPU-server-relative items in BIOS Setup for G431-MM1-GO. (Ac Loss Control, IOMMU, SMT Control)
  5. Fix LAN card MCX-354A-FCBT issue.
  6. Fix Qlogic QL45611HLCU MAC address issue in Legacy mode.
  7. Hide Setup unsupported xGMI speed option. ( 17G to 25G )
  8. Fix the lost characters issue on remote setup.
- 

### R33 (2021/02/04)

1. Update Redfish Inventory.
  2. Support System G431-MM1-GO.
- 

### R32 (2021/01/08)

1. Add SRIOV device Virtual bus support.
  2. Support Mellanox Connect-X6 to obtain LAN MAC in Legacy mode.
  3. Support Setup flash.
  4. Add pci option "PCIe x8" for SLSAS.
- 

### R31 (2020/12/03)

1. When PERR/SERR error is triggered, POST will show PERR/SERR error.(mantis 43326)
  2. Fix the problem that Micron 2200 NVMe cannot read and write.
  3. Fix multiple boot options after installing CentOS 7.8.
  4. Support Redfish Inventory.
  5. Support dump/restore Setup data from file.
  6. Fix PCI item issue caused by specific SKU name.
  7. Adjust PCI Subsystem item.
- 

### R30 (2020/10/16)

- 1 . Update AGESA version to 1.0.0.9.
  - 2 . Support Mellanox ConnexX5 MCX512A to obtain MAC address in Legacy mode.
- 

### R28 (2020/09/25)

1. Fix AC back after new LAN card make incorrect boot order issue before BMC 12.45.01
  2. Update CVE-2020-10713 secure boot key.
- 

### R27 (2020/08/21)

1. Fix the R25/R26 BIOS sometimes meet PMBUS data issue.
- 

### R26 (2020/08/14)

1. Update secure boot to resolve security issues (CVE-2020-10713).
  2. Fix 1P project R25 BIOS full DIMM issue.
  3. Adjust redfish boot order behavior.
  4. Adjust order of BIOS setup page of BMC Web
- 

### R25 (2020/07/20)

1. Update AGESA version to 1.0.0.8.
2. Add SMBIOS Type39.

## BIOS Release Notes

3. Remote BIOS support on BMC Web ( need BMC 12.44.04 or later ).
4. Fix Setup CSM can not modify problem.

---

### R23 (2020/06/18)

1. Fix the issue that AMD Radeon Instinct MI50 false detection to 4x4.
2. Add message frame for Real-time get bmc ip button.
3. Update SMBIOS Type130 Max speed / Real width.
4. Support Redfish remote setup secure boot.
5. Fix sometimes OS boot takes long time.
6. Fine tune remote setup function. (can adjust boot order via remote setup)
7. Add Intel Omni-path patch.
8. Add more UUID detection way.
9. Add "CSM Configuration" setup page.

---

### R22 (2020/05/08)

1. Update AGESA version to 1.0.0.7.
2. Adjust Format of BMC version.
3. Adjust default settings of Setup item "IOMMU" , "SMT Mode".
4. Adjust default settings of Setup item "MCA error thresh enable" , "MCA error thresh count".

---

### R21 (2020/04/28)

1. Fix the issue that BIOS flash tool can't update the non-boot area.
2. By default, the PXE boot option of the external NIC is started first.
3. Add UEFI logo output device option and set onboard VGA output by default.

---

### R20 (2020/03/20)

1. Update Redfish remote setup protocol.
2. Adjust boot option maximum.

---

### R19 (2020/03/02)

1. Increase the ECC Correctable Error Threshold Default.
2. Update TPM assurance AQ.
3. Fix Lan Mac Error for external lan card on system.

---

### R18 (2020/02/14)

1. Update AGESA version to 1.0.0.6
2. Adjust the behavior of IPMI boot device setting Legacy or UEFI
3. Adjust POST memory PMU error message
4. Add BIOS setup item "ERP mode" ( Need BMC support , Please check BMC version form web-site )

---

### R16 (2019/12/25)

- 1 . Update AGESA RomePI version to 1.0.0.5

---

### R15 (2019/12/06)

## BIOS Release Notes

1. Fix "Trigger memory single or multi bit error, BMC log have some problem." (mantis 39870, 38650, 38448, 38449)
  2. Add boot options for "Citrix Xenserver (Hypervisor)" and "VMware ESXi"
  3. Open BMC Virtual USB device list for BIOS setup (mantis 39856)
  4. Adjust SMBIOS type 10/41 information
- 

### R14 (2019/11/29)

1. Adjust Redhat 7 BIOS setup boot option (mantis 39000)
  2. Hide BMC Virtual USB LAN setup options (mantis 39856)
  3. Update VBIOS version to v110
- 

### R13 (2019/11/22)

1. Fix RTC default Year not same as BIOS build when clear CMOS (mantis 39641)
  2. Add NVIDIA GTX1080 Windows driver boot support
  3. Pass the USB Exposed Port System Test (mantis 40557)
- 

### R12 (2019/11/15)

1. Fix POST VGA resolution less than 1024x768 (mantis 40477)
  2. Hidden AMD PBS page item "SPI Lock"
  3. Fix ubuntu/rhel/windows show different information (mantis 39000)
  4. Fix the non-synchronization issue of items related to Console Redirection between BIOS Setup & Remote Setup.
  5. Adjust USB device tree.
  6. Display BMC version information on the POST log (SOL / Com port)
  7. Fix Mantis Issue #40556 USB3 Termination test fail.
- 

### R11 (2019/10/25)

- 1 . Update AGESA RomePI version to 1.0.0.4
  - 2 . Fix press F9 load default will show message in POST ( Mantis 39780 )
  - 3 . Fix BMC Virtual CDROM abnormal boot option name (mantis 39493)
  - 4 . Fix BMC detected PCIe SERR error log when install NVIDIA Tesla T4 ( Mantis 39622 )
  - 5 . Fix above 4G decode caused legacy LAN option rom exception (Mantis 39287)
  - 6 . Fix BMC will detect PCIe SERR error log when system reboot with NVIDIA Tesla V100. (Mantis 40268)
- 

### R10 (2019/10/09)

- 1 . Hidden un-use item ( CBS USB / HD Audio / NBIO FAN )
  - 2 . Fix Apacer DDR4 in BIOS setup show unkoown
  - 3 . Auto detect BMC vendor for hidden BMC LAN mode.
- 

### R09

- 1 . Fix "Upgrade BIOS does not show loading default message". (mantis 39780)
- 2 . When OS Clear TPM through BIOS, the related message will be displayed. (mantis 39942 / 38711 / 35798)
- 3 . Hide SPI TPM support options. (mantis 39944)
- 4 . Fix ""PCIE AER" enable, then XGMI speed will go to 16 gbps". (mantis 40195)

## BIOS Release Notes

- 5 . Fix "Found wrong sentence format in text mode". (mantis 39637)
  - 6 . Fix the issue that item "Power Policy Quick Settings" can't be adjusted by Remote Setup.
  - 7 . Fix the Load Default Function on the item "Power Policy Quick Settings".
  - 8 . Update VR(IR) version to A03.
- 

### R08

1. Fix NVMe Setup page display error for some systems.
  2. Fix some external LAN devices causing system errors.
  3. Fix ECC DIMM location error.
- 

### R07

1. Fix Mantis Issue #38500 SMBIOS UUID correction.
  2. Fix Mantis Issue #39650 M.2 detection.
  3. Update behavior for Power Policy Quick Settings "Standard".
  4. Adjust AC loss behavior. (BIOS load default will be synchronized to BMC)
- 

### R06

1. Adjust the behavior of the "Determinism Slider".
  2. Fix the problem that the BIOS version of SMBIOS type 0 can be modified.
  3. Add Power Policy Quick Settings item which controls CPU performance items Interlocking.
  4. BIOS setup item XGMI default string show Auto.
- 

### R05

1. Add Setup "AMD CBS" > "SMU Common options" > "Determinism Control": Enable > "Determinism Slider" power and performance related settings
  2. Disable Audio device for Server HLK
  3. Fixed CPU1 get wrong ECC location.
  4. Adjusted SEL sensor number.
- 

### R04

1. Update AGESA version to 1.0.0.2
  2. Adjust DRAM ECC SEL Log
  3. Disable this feature if the BMC does not support Redfish
  4. Fixed can not boot Windows when enable "Enable AER Cap" item issue
- 

### R03

- 1 . Fix Windows HLK TPM 2.0 preboot interface test failed.
  - 2 . Adjust low temperature setting
  - 3 . Fix some BIOS setup item can't be remote setup issue.
  - 4 . Fix random hang BIOS setup issue.
  - 5 . Add Interlock function by Determinism Slider.
- 

### R02

- 1 . Support for future BMC version of Redfish and Remote Setup.
-

# BIOS Release Notes

## R01

- 1 . Adjust memory ECC behavior.
  - 2 . Adjust BMC FW version format.
  - 3 . Fix NVMe does not display POST and BIOS (Mantis 38812)
  - 4 . Fix PCB 1.x board xGMI default max speed is not 10.667Gbps.
  - 5 . Add wait BMC ready setup item.
- 

## T09

- 1 . Default XGMI 10.6G for PCB 1.x.
  - 2 . Post shows CPU spec speed not current speed.
  - 3 . Fix BMC IPv6 address cannot show on setup.
  - 4 . Set power limit default value as 300w.
- 

## T08

- 1 . Fine Setup main page.
  - 2 . Fix auto enter recovery mode issue for 32MB BIOS with Rome CPU.
- 

## T06

1. BIOS setup menu show “CSM configuration” page
  - 2 . Support Intel i350 PXE driver
  - 3 . Increase I2C hold time.
  - 4 . Add CPU information on BIOS setup main page
  - 5 . Update CPU SATA controller setting.
- 

## T05

- 1 . Update VR(IR) version to A02
- 

## T04

- 1 . Update AGESA version to 0.0.9.0
  - 2 . Fix not found LAN x550 option rom and MAC address N / A issue.
    - 3 . Support BMC Web UI PCI information show link speed and link width.
    - 4 . Fixed an issue where the External LAN card on the BMC Web UI does not have a MAC address.
  - 5 . Fixed SMBIOS type 9, type 41 garbled issue.
- 

## T03

First release.