

BIOS Release Notes

TITLE

SUBJECT: MD71-HB0 BIOS Release Notes version [R25](#)

System: [NA](#)

About This Release

Build Date: [2024/11/21](#)

BIOS Checksum: [0xCAD89FA8](#) (16M), [0x8EF62EAA](#) (32M)

Release Owner: richard.huang

BIOS Components/Contents

Processor stepping(s) supported: Intel® Skylake-SP/Cascadelake-SP processors

System hardware configurations supported: MD71-HB0

Microcode updates versions:

CPUID	Family	Microcode Update ID
50653	SkyLake-Server Processor B-1	01000191
50654	SkyLake-Server Processor H-0	02007006
50655	CascadeLake-Server Processor A-0	03000012
50656	CascadeLake-Server Processor B-0	04003801
50657	CascadeLake-Server Processor B-1	05003801

IPMI support:

AMI Kernel version: [Gbt_Kernel_064_01](#)

Intel CSI/MRC Package version: [0630.P12](#)

SPI Descriptor version: [04.01.05.105.0](#)

OPROM version :

BIOS Release Notes

OPROM	Version
AST2500 VGA	1.09.00
INTEL 10G LAN EFI	7.0.19
INTEL 1G PXE	1.5.53
INTEL 10G PXE	2.3.24
INTEL 1G LAN EFI	8.5.21
INTEL RAID PACKAGE	RSTe 6.2 PV

Installation Notes

IMPORTANT NOTES:

1. Please extract the MD71-HB0_ [R25](#).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 Version CHECK INSTRUCTIONS:

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

Known Issues/Workarounds

Issues fixed in this version

BIOS Release Notes

R25

1. [Feature] 1. Update RC 0630.P12 (2025.1 IPU PV)
 2. Update Microcode CLX B0 - MBF50656_04003801.pdb and CLX B1 - MBF50657_05003801.pdb
 3. Update SPS_E5_04_01_05_105_0
 4. Update for Intel Security:
INTEL-SA-01153: CVE-2024-28956
INTEL-SA-01139: CVE-2024-28047
 5. Update for AMI Security:
SA50258: CWE-190, iSCSI Remote Memory Corruption and Dos.
SA50158: CWE-269, UEFI Variable Access - PlatformLang and Timeout
-

R24

1. [Bug Fix] Fix pkfail issue.
-

R23

1. [Feature] 1. Update RC 0629.P09 (2024.3 IPU PV)
 2. Update microcode CLX B0 - MBF50656_04003707.pdb and CLX B1 - MBF50657_05003707.pdb
 3. Update BIOS SINIT ACM version 1.7.57
 4. Update for [Security] Vulnerabilities in EDK2 NetworkPkg include : CVE-2023-45236, CVE-2023-45237
-

R22

1. [Bug Fix] 1. Update for security of LogoFAIL vulnerability include following
CVE-2023-39538, CVE-2023-39539
-

R21

1. [Bug Fix] Update for security of PixieFail: vulnerabilities in Tianocore's EDK II IPv6 network stack include following
CVE-2023-45229, CVE-2023-45230, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235
-

R20

1. [Feature] 1. Update RC 0628.P59 (2024.1 IPU PV)
2. Update microcode SKX B1 - M9750653_01000191, CLX B0 - MBF50656_04003605, CLX B1 - MBF50657_05003605
3. Update BIOS ACM version v1.7.55 and SINIT version 1.7.56
4. Update for security INTEL-UA-00985

BIOS Release Notes

5. Update for security AMI SA50198: CVE-2022-36763, CVE-2022-36764

AMI SA50197: CVE-2022-21894

AMI SA50179: CVE-2021-38575

AMI SA50202: CVE-2023-34470

AMI SA50205: CVE-2023-39537

AMI SA50191: CVE-2023-0465

AMI SA50193: CVE-2023-0464

R19

1. [Feature] 1. Update RC 0628.P50 (2023.3 IPU PV)
2. Update microcode SKX B1 - M9750653_01000181, SKX H0 - MB750654_02007006, CLX B0 - MBF50656_04003604, CLX B1 - MBF50657_05003604
3. Update SPS_E5_04_01_05_002_0
4. Update for security INTEL-SA-00828: CVE-2022-40982
5. Update for security INTEL-SA-00813: CVE-2022-43505
6. Update for security AMI SA50170: CVE-2021-38578

R18

1. [Feature] Update for fix security AMI SMI vulnerabilities of
 - [1] Improper size validation of SMM Communication Buffer
 - [2] Improper validation when reading and writing UEFI Variables

R17

1. [Feature] Update RC 0626.P01 (2023.1 IPU PV)
2. [Feature] Update microcode SKX-H0: MB750654_02006E05, CLX-B0: MBf50656_04003303, CLX-B1: MBf50657_05003303, SKX-B1: M9750653_01000161
3. [Feature] Update SPS_E5_04.01.04.901.0
4. [Feature] Update for security INTEL-SA-00717: CVE-2022-32231, CVE-2022-26343
5. [Feature] Update for security AMI SA50162: CVE-2022-34301, CVE-2022-34302, CVE-2022-34303
6. [Feature] Update for security AMI SA50153
7. [Feature] Update for security AMI SA50121: CVE-2021-33164

R16

1. [Feature] Update 2022.1 IPU for security INTEL-SA-00616: CVE-2021-21131, CVE-2021-21136; INTEL-SA-00601: CVE-2021-0189, CVE-2021-0159, CVE-2021-33123, CVE-2021-33124.

R15

1. [Feature] Update RC 0616.D08 (2021.2 IPU PV)

BIOS Release Notes

2. [Feature] Update microcode SKX-H0: MB750654_02006c0a, CLX-B0: MBf50656_0400320a, CLX-B1: MBf50657_0500320a
 3. [Feature] Update BIOS ACM v1.7.51 / SINIT v1.7.51
 4. [Feature] Update DCPMM UEFI Driver v01.00.00.3531
 5. [Feature] Update SPS_E5_04.01.04.601.0
 6. [Bug Fix] Update for security INTEL-SA-00532, INTEL-SA-00527, INTEL-SA-00525, INTEL-SA-00470
-