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 © 2023 Super Micro Computer, Inc. All rights reserved.*

Product Name	**X13SEM-(T)F**
Release Version	**1.4**
Release Date	**08/10/2023**
Build Date	**08/10/2023**
Previous Version	**1.3**
Update Category	**Recommended**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Updated Intel BKC SPR 2023_WW21 PLR2/3, EMR 2023_WW25, Intel RC Version 103.D70.** **2. Updated Seamless MCU capsule revision to 1.0b for PLR2/3.** **3. Updated Intel Server Platform Services SPS_E5_6.0.5.046 PLR3 HF for Eagle Stream Server.** **4. Fixed SUM RoT power fail malfunction issue.** **5. Exposed PCIe port control. Users used it to save power for SPR MCC or SPR-EE LCC speed restore.** **6. Modified Me version strings, remove the "Manufacturer ID" string.**
New features	**N/A**

Fixes	1. **Fixed missing end tag (0x78) of VPD data when the VPD length is multiple of 4. (0 base)** 2. **As RTC power loss ever happens, configure BIOS build time to system time.** 3. **Memory speed should be MT/s not MHz.**

Release Notes from Previous Release(s)

1.3 (05/25/2023)

1. *Updated Intel BKC 2023_WW13, Intel RC Version 100.D45 PLR1.*
2. *Enhanced the solution for the error/warning message from dmidecode after a modification by AMIDE.*
3. *Revised the PCIe port naming under IIO Configuration.*
4. *Updated ME XML override python script for SPR and EMR build.*
5. *Enhanced the no bootable device message on POST screen feature.*
6. *Exposed "Opt-Out Illegal MSI Mitigation," hid "RestoreROWritePerf" settings from the IIO configuration.*
7. *Added onboard M.2 slots to the VMD-capability table.*

1.1 (01/04/2023)

1. Updated AMI label to 5.29_EagleStreamCrb_0ACOR_071_ BETA.
2. Exposed and adjusted MRRS item for Gen5 performance fine tune.
3. Fixed the FWTS and WHQL fail issue.
4. Updated the VROC SATA/sSATA EFI driver to VROC PreOS v8.0.0.4006 PV.
5. In order for the code base of SuperBIOS and AMI to be compatible, use Supermicro's defined GUID for passing the variable to BMC.
6. Fixed Type 17 so that it will not follow SPD Spec MemoryChannelBusWidth.
7. Exposed the CPU's "Optimized Power Mode" feature.
8. Updated the SATA SGPIO Mode option strings for all SATA configuration menus.
9. Hid the "Homeless Prefetch" feature.
10. Removed the VMD function.
11. Added CXL related setup items.
12. Removed VMD mode.
13. Supported two new NVMe 1U SKU (CN2 to NVMe, CN3 to 1U RSC slot2).
14. Revised inter-Group of Legacy which can't be ordered.
15. Fixed the BIOS IIO Configuration menu so that it will display four CPU socket menus when loading BIOS Optimized Defaults issue.
16. Fixed the WHQL HSTI Rollback firmware error.
17. Fixed the issue where the CPU2 TDP disappears in BMC web.
18. Corrected BankLocator for DP 1SPC projects.

1.0b (11/04/2022)

1. Updated AMI label to 5.29_EagleStreamCrb_0ACOR_066.
2. Enabled SUM command GetBiosCfg to get the current bioscfg after booting to the setup menu.
3. Updated the EfiOsBootOptionNames module to label 19.
4. Enabled the AFU to work using the /N or /clnevnlog commands.
5. Added the TOKEN "SMC_HECI_HIDE_DELAY" to control the HECI-x.
6. Enhanced the following:

   a) Created an individual module named "SmcKMSOOB" that prepares the VFR/UNI and creates the ConfigAccess Protocol.
   b) Commented out the declaration of "Supermicro KMIP Form" in the table "AllowedHpkTable" in the file SmcOobPlatformPolicySetting.c so that only one page of the "Supermicro KMIP Form" is generated in the BIOS Config XML.

7. Added UEFI OS name automatically for removable device (USB key).
8. Removed the "Supermicro Security erase" page from HII format.
9. Enhanced the following:

   a) Added SecureBoot database to meet Redfish specification.
   b) Added Delete Single key function.

10. Added the BIOS POST progress support requirement in Redfish.
11. Enabled program the NVRAM using the AFU utility by correcting the gPayloadOffset definition.
12. Added support for the VPP interrupt mode on rev1.02 m/b.
13. Set the BIOS_EXIT_UBOOT/BIOS_BOOT_OK at the end of POST.
14. Fixed the password to be saved after the NVRAM module is updated to label 26.
15. Fixed the SMBIOS type 17 memory serial number to match the memory DIMM bar code.
16. Fixed the SUM DMI data update to set every DMI value

1.0a (08/23/2022)

1. *Updated AMI label to 5.28_EagleStreamCrb_0ACOR_059_BETA.*
2. *Updated USB ports mapping.*
3. *Added VPP_POLLING_MODE to support motherboard designs without VPP Alert.*
4. *Enabled the SUM TC: 220/271/356/457 to boot Windows OS after flashing the BIOS.*
5. *Changed the string from "Memory Health Components" to "Enhanced PPR."*
6. *Synchronized the chassis type from FRU0 to SMBIOS Type 03.*
7. *Enabled the setting "CPU C1 auto demotion" to be disabled.*
8. *Updated VROC SATA/sSATA EFI driver to VROC PreOS v8.0.0.1336.*
9. *Fixed the ability to clear event logs.*

1.0 (5/16/2022)

Initial Release.