BIOS Release Notes Form

Product Name	**X13DEM**
Release Version	**3.0 SPS: 6.1.4.215**
Build Date	**04/08/2026**
Previous Version	**2.8 SPS: 6.1.4.215**
Update Category	**Recommended**
SMC Best Known BIOS/BMC/SAA Combination Ver	**BIOS: 3.0** **BMC: 01.09.15** **SAA: 1.5.0-p3**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Updated the BIOS version to 3.0.** **2. Updated secure boot DB to add a new Microsoft certificate.** **3. Exposed Telco NFVI, Telco NFVI-FP, and Telco FlexRAN workload profiles.** **4. Updated the code base to 5.32_EagleStreamCrb_0ACOR_114.** **5. Updated HddSecurity for SA50336 Security Advisory to address CVE-2025-58772 (8.2 High) and updated TcgStorageSecurity for SA50336 Security Advisory to address CVE-2025-58774 (8.3 High).**
New features	**None**
Fixes	**1. Security issue (PB:222344).**

	2. **Fixed how IPv6 HTTP Boot via the manual BOOT URI was not working.**

Release Notes from Previous Release(s)

2.8 SPS: 6.1.4.215 (11/25/2025)

1. *Updated the BIOS version to 2.8.*
2. *SmcOOBV2.01.11 was updated.*
3. *Exposed the "Provision Factory Defaults" setup item for SAA.*
4. *Updated the code base to (BETA)5.32_EagleStreamCrb_0ACOR_112.*
5. *VROC PreOS was updated.*
6. *Resolved an issue where the BIOS did not report the Type 40 structure when the AOC VPD size exceeded the expected limit (e.g., AOC-S200G-B2C-O).*
7. *Fixed an issue where the SAA changebioscfg and IPMI command was used to force PXE boot at the same time, and the system would not boot into PXE.*

2.7 SPS: 6.1.4.204 (07/11/2025)

1. *Updated AMI 5.32_EagleStreamCrb_0ACOR_110 for IPU2025.3.*
2. *Updated Intel #855697 Intel Server Platform Services SPS_E5_06.01.04.204.0 Release for IPU 2025.3 PV Eagle Stream Refresh Server.*
3. *Enhanced the patch for AOC-SMG4-2M2.*
4. *The patch system randomly hangs during a boot into Windows 2022 OS.*
5. *Updated secure boot DBX for CVE-2025-3052.*
6. *After a boot override, the boot order changed and efibootmgr could not be saved.*
7. *Implemented the TPM EK ECC certificate feature.*
8. *Fixed the issue when using Redfish API to read the BIOS config, it had an empty menu name.*
9. *Patch SMBIOS was not ready before hooking the system diagnostics.*

2.6 SPS: 6.1.4.89 (05/15/2025)

1. *Updated AMI 5.32_EagleStreamCrb_0ACOR_108_BETA for IPU2025.2.*
2. *Implemented the TPM EK public certificate feature.*
3. *Removed the warning message, "Crystal Ridge is not support."*
4. *Updated Secure Boot DBX to address the AMI SA50300 (CVE-2024-7344\CVE-2023-24932 (8.2 High/6.7 Middle)) security issue.*
5. *Updated Intel-Restricted-2025-2-IPU 20250324_20252IPU Release.*
6. *Exposed the "Enable SAF" item.*
7. *Updated uPLR3 OOB.*
8. *Changed the CPU core disable BIOS format from it being by bitmap to it being by core number.*
9. *Added a patch for AOC-SMG4-2M2 due to how this AOC could not support SMC FRU detection design.*

2.5 SPS: 6.1.4.75 (02/05/2025)

1. *Updated AMI label to 5.32_EagleStreamCrb_0ACOR_107_BETA for uPLR3.*
2. *Exposed PCI-E Completion Timeout.*
3. *Added a BIOS patch for the issue about executing PPR with warm reset system hang.*
4. *Added a MKTME/CPU 46Bits PA dependency message to avoid confusing customers.*
5. *Exposed "Secure Boot Mode" setup item to SAA.*
6. *Updated Seamless MCU capsule revision to 2.4 for EMR 2.5 BIOS (UPLR3).*
7. *Support added to report TDP calculation parameter and MAX power calculation parameter for the 32 Gb BASE memory chip.*

8. *Default enabled LOAD_IMAGE_PATCH for the issue where cburn failed on/off.*
9. *Implemented the TPM Redfish MeasurementSet feature.*
10. *Updated the SmcOob module to SMCOOBV2.01.06 to hide the duplicate items when it was not in the exposed page.*
11. *Hidden the SmcSecureBoot page policy.*
12. *Fixed how the DNS IP was shown incorrectly when the DNS IP was set in the web.*
13. *Runtime updated the smbios date to ROMHOLE.*
14. *Fixed how there was no copyright string in text mode.*
15. *Fixed how the system went to the wrong setup menu when boot mode set to "DUAL" and "Legacy To Efi" was enabled.*
16. *Fix how Rocky OS RAID 1 couldn't boot.*
17. *Fixed how the BMC IPV6 setup items didn't work.*
18. *Fixed how AOC couldn't be detected when it was using x4x4 Bifurcate.*
19. *Fixed the problem with HttpBootCheckSpaceToDeleteAllHttp.*

2.4 SPS: 6.1.4.75 (09/23/2024)

1. *Updated AMI label to 5.32_EagleStreamCrb_0ACOR_105 uPLR2 OOB.*
2. *Updated BIOS revision to 2.4.*

2.3 SPS: 6.1.4.47 (06/04/2024)

1. *Updated AMI label to 5.32_EagleStreamCrb_0ACOR_103 uPLR1 OOB.*
2. *Fixed the issue where the MAC address in tag V4 and V5 was incorrect when installing the Broadcom quad-port network adapter(BCM957504-N425G).*
3. *Patch for Mellanox InfiniBand Controller MAC Address retrieval issue.*
4. *Updated AMITSE module for AMI SA50216.*
5. *Updated AMITSE module for AMI SA50230.*
6. *Updated EDK2 NetworkPkg for AMI SA50218.*
7. *Updated BIOS revision to 2.3.*
8. *Added FixedBootOrder Group boot device default value.*
9. *Updated the SUM OOB module to SMCOOBV2.00.22 to support Redfish replacing the display name feature.*
10. *Fixed how the BIOS Setup could not set stateful mode of IPv6.*
11. *Read CPU CAP ID to get VROC key activation status and decide on VMD auto mode.*
12. *Enabled "Disable BIOS Done" in Factory Mode.*
13. *Implemented Workload Profile function.*
14. *Revised the error message for MINOR_ERR_INVALID_TOPOLOGY.*
15. *BIOS only reported network device VPD.*
16. *Exposed "Directory Mode Enable" and add X-AMI.*
17. *Set Chassis type in SMBIOS to default (0x11) when Chassis type from FRU was 0x00 or 0xFF.*
18. *Removed the report from the unused boot device group in the Redfish BBS.*
19. *Added X-AMI for "Disable Bitmap" under "CPU1 Core Disable Bitmap" and "CPU2 Core Disable Bitmap" page.*
20. *[SmcSecureBoot] Updated Supermicro Secure Boot Main setup items X-AMI ID to match the Mapping Language Golden Sample.*
21. *Improved SmcVPD third-party LAN card's function.*
22. *Updated Seamless MCU capsule revision to 2.2 for EMR 2.3 BIOS (UPLR1 OOB).*
23. *Updated the options for the "BMC LAN Selection."*
24. *Modified "Virtual NUMA" string.*

25. *Added feature that enables VMD when Intel On Demand is activated for EMR CPU.*
26. *Fixed the system hang during IPv4 HTTP boot.*
27. *Fixed the SUM GetBiosCfg command failed issue.*
28. *Fixed how the X710 FW information did not show correctly in BIOS setup.*
29. *Fixed how CX6 LAN card's VPD data couldn't fill in type 40.*
30. *Fixed how EFI OS boot order was not first, if the issue was BMC changing the boot order (one time), then install EFI OS by PXE.*
31. *Overwrote AmiPcdChassisType to sync SYS_CHASSIS_TYPE_1 setting.*

2.1a SPS: 6.1.4.5 (03/20/2024)

1. *Only applied HW VRM patch for 1.10 MB.*
2. *Updated BIOS revision to 2.1a.*

2.1 SPS: 6.1.4.5 (8/25/2023)

1. *Updated AMI label to 5.32_EagleStreamCrb_0ACOR_099_Beta for BKC WW47 EMR PV candidate.*
2. *Updated Eagle Stream Refresh Emerald Rapids Unified Patch Engineering Release - 2023 WW47.*
3. *Updated VROC SATA/sSATA/tSATA/VMD EFI driver to VROC PreOS v8.5.0.1096 PC.*
4. *Added VROC on Demand driver support.*
5. *Updated the SUM OOB module to SMCOOBV2.00.21 to support Redfish to replace the display name feature.*
6. *Used PCIe ASPM Support (Global) to control ASPM(PCH), PCI-E ASPM Support(IIO), Native ASPM(ACPI) option.*
7. *Hid "XPT Prefetch" in EMR CPU.*
8. *Supported VPD data of Broadcom Network Adapter.*
9. *Greyed out "Preferred DNS server IP" and "Alternative DNS server IP".*
10. *Implemented BIOS setup keyword search function.*
11. *Fixed HostInterface On/Off stress test that will drop in UEFI Shell intermittently.*
12. *Changed the FixedBootOrder BBS Group define start from COMMNE00 not COMMNE01.*
13. *Updated secure boot KEK/DB to add new Microsoft certificate.*
14. *Added X-AMI for "Disable Excluding Mem Below 1MB In CMR" and "TME-MT/TDX Key Split", and updated the strings to Camel-Case format.*
15. *Exposed "Page Policy".*
16. *Updated built-in SuperDiag to fixed issues, based on GIT_c4cc82130966861f501de64bd6bc4472ed05b2a5.*
17. *Default disabled OOB send replace DisplayName feature to avoid the SUM OOB test fail problem.*
18. *Made sure to assign a unique ID for NVME device.*
19. *Cleared RTC clear flag and IPMI RTC clear flag individually to prevent "Setup default has been loaded" still being displayed during next boot.*
20. *Resolved how IPV6 "Preferred DNS server IP" and IPV6 "Alternative DNS server IP" were not being displayed correctly on BIOS setup.*
21. *Fixed Secure erase malfunction.*
22. *Resolved the "BMC LAN Selection" setup item differing from the "LAN selection interface" under BMC WEB GUI.*
23. *Resolved how even if the 'Ipv6' is disabled in the BMC WEB GUI, the IPv6 address was still being displayed during the EarlyVideo stage.*
24. *Fixed when installing AOC-S25GC-I2S on RSC-H-66G5L slot1, the network driver will show "Disconnect" under the BIOS page issue.*

1.4 SPS: 6.0.5.46 (8/25/2023)

1. *Updated AMI label to 5.31_EagleStreamCrb_EMR_0ACOR_087.*
2. *Fixing the information of "Available Bitmap:" cannot be found in the BIOS Cfg file.*
3. *Updated BIOS revision to 1.4.*
4. *Updated Intel Server Platform Services SPS_E5_6.0.5.046 PLR3 HF for Eagle Stream Server Update 782193 Intel Server Platform Services SPS_E5_6.0.5.046 PLR3 HF for Eagle Stream Server.*
5. *Modified ME version strings, removed the "Manufacturer ID" string.*
6. *Fixed the missing end tag (0x78) of VPD data when the VPD length is multiple of 4. (0 base)*
7. *Expose the SATA1 menu for the PCH SATA M.2 setting to fix cannot enable RAID mode for the SATA M.2 device problem.*
8. *Memory speed should be MT/s, not MHz.*
9. *Fixed NVMe hot-plug malfunction on SYS-121H-TNR's last 8 ports issue.*

1.3 SPS: 6.0.4.70 (6/1/2023)

1. *Updated Intel BKC SPR 2023_WW13 PLR1, EMR 2023_WW19, Intel RC Version 101.D66.*
2. *Enhanced the solution for the error/warning message from dmidecode after a modification by AMIDE.*
3. *Removed first capital letter S from Micron type 17 serial number.*
4. *Updated options of Enhanced PPR from Disabled/Once/Persistent to Disable/Enable/Persistent.*
5. *Added support for 3'rd lan card VPD.(Mellanox)*
6. *Exported PCIe leaky bucket related items and add X-AMI ID.*
7. *Support SYS-121H-TNR with one BPN only sku.*
8. *Kept HBM SMBIOS type 17 structures.*
9. *Set PPIN default value to Unlock.*
10. *Rolled back GPNV module to fix type 15 disappear.*
11. *Added SuperDiag Launcher driver.*

1.1 (1/20/2023)

1. *Updated AMI label to 5.29_EagleStreamCrb_0ACOR_071_BETA.*
2. *Updated SPS 6.0.4.25.*
3. *Updated 806F8 Intel(R) Processor SPR E-Stepping microcode 2B000161 and HBM B-Stepping microcode 2C000120.*
4. *Updated BIOS revision to 1.1.*
5. *Exposed "CXL Security Level" and "CXL Header Bypass" for CXL.*
6. *Enhanced memory map out feature.*

1.0a (11/2/2022)

1. *Updated Intel BKC 2022 WW43 (KIT #750947, Intel RC Version 90.D03).*
2. *Updated BIOS revision to 1.0a.*
3. *Supports SYS-221HE-FTNR system configuration.*
4. *Set PCIe PLL SSC enabled value from 0.3% to 0.5%.*
5. *Fixed AFU return error so it will stop running when using the /N or /clnevnlog command.*
6. *Followed Intel WW36 MOW to disable Pre-GO_S1 setting.*
7. *Followed BMC_Network_AOC_Monitoring_Spec_v2.2 to discard the action to send AIOM/AOC IO Module LAN MAC to BMC.*
8. *Updated SPS 6.0.3.271 2S PC Hotfix Release for Eaglestream Platforms*
9. *Added new feature to set BIOS_EXIT_UBOOT/BIOS_BOOT_OK at end of POST.*

10. Fixed SST function, not work issue.
11. Fixed the memory serial number of SMBIOS type 17, did not match memory DIMM bar code.

1.0

1. First release.