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 © 2018 Super Micro Computer, Inc. All rights reserved.

Product Name	**X12DPT-B6**
Release Version	**2.3 SPS: 4.4.4.702**
Build Date	**03/29/2025**
Previous Version	**2.2 SPS: 4.4.4.702**
Update Category	**Recommended**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Updated the kernel to 5.22_WhitleyCrb_0ACMS_ICX_082 (IPU 2025.2 PV).** **2. Applied SA50300 to address the CVE-2024-7344 (High, 8.2) security issue.** **3. Removed the warning message, "Crystal Ridge is not support."** **4. Applied AMI SA50288 to address OpenSSL MbedTLS (CVE-2023-52353) and Elliptic Curve API (CVE-2024-9143) vulnerabilities.** **5. When enabling block SID, set AUTO_ACCEPT_PPI to avoid having to wait for user acceptance before continuing.**
New features	**None**

Fixes	**1. If http boot was ever configured on the BIOS setup or via SUM, skip the boot order update.** **2. Updated the boot order by UEFI/legacy/dual boot category and boot option sequence to reflect HW configuration before referring to it.** **3. Fixed the issue where the built-in UEFI shell resulted in no mapping found after enabling Legacy to EFI support and setting boot mode to Dual mode.**

Release Notes from Previous Release(s)

2.2 SPS: 4.4.4.702 (10/24/2024)

1. *Updated kernel to 5.22_WhitleyCrb_0ACMS_ICX_081 (2025.1 IPU PV).*
2. *Applied SA50230 supplement (Image Parser Corruption Vulnerability).*
3. *Applied SA50218 supplement (Vulnerability In EDK2 NetworkPkg).*
4. *For SA50243 (CVSS3.1 (7.5, High)), fixed how the UsbRtSmm module had a TOCTOU vulnerability.*
5. *Applied SA50235 for extended parser corruption correction.*
6. *Applied AMI SA50232 to address the security vulnerabilities listed below.*
    a. *CVE-2023-45236 Use of a Weak PseudoRandom Number Generator (Risk Level : 5.8).*
    b. *CVE-2023-45237 Predictable TCP initial sequence numbers (ISNs) generated by the TCP/IP stack (Risk Level: 5.3).*
7. *Enhanced ErstWriteErrorRecord () and ErstReadErrorRecord () for security vulnerabilities (Refer to EagleStream SVN 3722).*
8. *Set the Chassis type in smbios to default (0x11) when the Chassis type from fru was 0x00 or 0xFF.*
9. *Saved MAC to PCD for filling DUID with UUID (Refer to EagleStream SVN 3621 and 3622).*
10. *SMBIOS type 40 VPD update.*
11. *Exposed PCI-E Completion Timeout.*
12. *Removed VLAN callback function in Setup BMC page.*
13. *Removed setup callback relative to BMC Network Configuration (Refer to EagleStream SVN 3833).*
14. *Runtime updated smbios date to ROMHOLE (Refer to EagleStream SVN 3839).*
15. *Resolved IPMI PXE boot fails after installing OS.*
16. *Resolved how the boot order could not be adjusted by AMI SCE.*
17. *Overwrote AmiPcdChassisType to sync SYS_CHASSIS_TYPE_1 setting.*
18. *Kept boot mode during IPMI force boot.*
19. *Fixed how there was no copyright string in text mode.*

1.9 SPS: 4.4.4.603 (01/11/2024)

1. *Exposed "Pre-boot DMA Protection".*
2. *Applied SA50216 supplement.*
3. *Fixed how the HostInterface On/Off test will drop in 4x times in UEFI Shell.*
4. *Resolved how CPU2 TDP on BMC WebUI displays 0 sometimes (Refer to EagleStream SVN 1919).*
5. *Resolved how the KMS configuration could not be preserved after load BIOS default.*
6. *Displayed dynamic gateway IPV6 address as "::::::::" on BIOS setup if dynamic router info set count is 0.*
7. *Displayed static gateway IPV6 address as "::::::::" on BIOS setup if could not get valid gateway IPV6 address through IPMI.*

1.8 SPS: 4.4.4.603 (11/22/2023)

1. *Updated source base to 5.22_WhitleyCrb_0ACMS_ICX_077 (2024.1 IPU-PV).*
2. *Fixed system stuck at 0xB2 when plugging BPS with MM mode.*
3. *Grayed out "Preferred DNS server IP" and "Alternative DNS server IP".*
4. *Updated secure boot KEK and DB.*
5. *Updated Intel Server Platform Services for Whitley Server Platforms IPU2024.1 4.4.4.603.*
6. *Updated Dx/Mx PC microcode Intel-Restricted-2024-1-IPU-20231009_20241IPU for IPU2024.1.*
7. *Fixed ATT Test case "Check BBS test" failed when using Windows OS for test problem.*

1.7 SPS: 4.4.4.500 (09/24/2023)

1. *Updated 5.22_WhitleyCrb_0ACMS_ICX_076 (IPU-PV 2023.3).*
2. *Updated Intel Server Platform Services for Whitley Server Platforms IPU2023.3 4.4.4.500.*
3. *Fixed 3rd card VPD data can't be collected completely.*
4. *Added SEL for UPI (topology change) link degraded.*
5. *Updated BMC/BMC Network Configuration page IPv6 DNS/DNS2 setting.*
6. *Updated USB keyboard code to fix scanner input issue.*
7. *Changed the strings from "Lock mode" to "Lockdown mode".*
8. *Updated x-AMI ID for PCH VMD mode.*
9. *Updated Dx/Mx BETA microcode for IPU2023.4 Out of band for Intel-TA-00950.*
10. *Fixed an issue where UECC mapped out DIMM information that had to be removed by clearing CMOS.*
11. *Fixed the issue that SMBIOS Type0 System Family change could not be preserved after clearing CMOS.*
12. *Fixed system hang on 0xA9 when installing large MMIO request AOC on system such as AOC-A25G-i4SM.*
13. *Fixed DIMM total memory size, which is shown incorrectly in the setup.*
14. *Fixed ENERGY_PERF_BIAS_CFG Mode item change to default after SUM update BIOS with --preserve_setting command.*
15. *Resolved IPV6 "Gateway IP" is not displayed correctly on the BIOS setup.*

1.5 SPS: 4.4.4.301 (3/28/2023)

1. *Updated 5.22_WhitleyCrb_0ACMS_ICX_075 Intel 2023.2 IPU-PV, please check the header for firmware revisions.*
2. *Pulled high GPP_C10_FM_PCH_SATA_RAID_KEY first before VROC key detection.*
3. *No boot option for single HDD under RAID mode.*

1. *Fixed system hang on 0xA9 after setting MMCFG base to 1.5G and 1.75G.*
2. *Fixed the SUM TC: 2020 test fail problem.*

1.4b (1/12/2023)

1. *Updated 5.22_WhitleyCrb_0ACMS_ICX_74 Intel BKCWW46 IPU2023.1. Please check the header for firmware revisions.*
2. *Updated VROC SATA/sSATA EFI driver to VROC PreOS v7.8.0.1012 in order to address Intel Virtual RAID on CPU (VROC): Data Loss Exposure Due to RAID 5 TRIM Support. (Document #737276)*
3. *Moved AF w/a code.*
4. *Updated DBX file to fix Secure Boot Bypass issue.*
5. *Updated for template v1.1_20220809.*
6. *Updated BPS UEFI driver to 02.00.00.3887 for IPU2022.3.*
7. *Followed the SMBIOS template to sync the chassis type from FRU0 to SMBIOS Type 03.*
8. *Updated Intel Server Platform Services for Whitley Server Platforms IPU2023.1 4.4.4.301*
9. *Corrected PayloadOffset definition to fix the inability to successfully program NVRAM with AFU utility.*
10. *Enhancements when running the SUM TC: 220/271/356/457/2071/3056/4057 with Windows OS will cause the boot order to compare fail after flash BIOS.*
11. *Fixed an issue where runtime memory errors were not being reported in the SMBIOS event log.*

1.4a (1/30/2022)

1. *Updated Intel BKC PLR1.*
2. *Enabled boot guard.*
3. *Changed revision to 1.2.*
4. *Changed revision to 1.4.*
5. *Updated OOB preserve function.*
6. *Updated Intel BKC to PLR3.*
7. *Fixed NVMe hotplug problem that was due to a wrong value programmed in CPLD GPIO9.*
8. *Added Intel BKC Version 2022_WW46 (KIT #750969).*
9. *Added Central Park Intel® Central Park Whitley Release 30P19.*
10. *Added ME-SPS Firmware SPS_E5_04.04.04.301.0.*
11. *Added RSTe PreOS Components 7.8.0.1012.*
12. *Added VMDVROC_1.efi 7.8.0.1012.*
13. *Added VMDVROC_2.efi 7.8.0.1012.*
14. *Added ACM Binaries BIOS ACM v1.3.6/ SINIT ACM v1.3.7.*
15. *Added Jacksonville 1 GbE NVM _I219_Nahum7_Purley_LM_No-LAN-Switch_Rev0.2.*
16. *Added Microcode Version IceLake CPU LCC MCU: m_97_606a0_80000031.mcb.*
17. *Added IceLake CPU HCC MCU: m_87_606a4_8b0003f0.mcb.*
18. *Added IceLake CPU XCC C0 MCU: m_87_606a5_8c0002f0.mcb.*
19. *Added IceLake CPU XCC D0 MCU: m_87_606a6_8d000280.mcb.*
20. *Added IceLake CPU HCC Production MCU: m_87_606a4_0b000280.mcb.*
21. *Added IceLake CPU XCC C0 Production MCU: m_87_606a5_0c0002f0.mcb.*
22. *Added IceLake CPU XCC D0 Production MCU: m_87_606a6_0d000389.mcb.*
23. *Added DCPMM UEFI and HII Driver v02.00.00.3887.*

1.2 (2/12/2022)

1. Removed 1G option from MMCFG base to avoid system hang.
2. Fixed the SMBIOS event log ERROR CODE not displaying correctly under BIOS menu issue (EFI error type).
3. Added "Preserve_SMBIOS", "Preserve_OA" into FlashFlag when in the condition "NvramDefaultMode".
4. Fixed the setup item "Lockdown Mode", which is always gray-out.
5. Fixed SpeedStep (P-States) setting change when its default setting is set to Disabled and load BIOS defaults in Setup.
6. Rolled back physical slot number settings to 1.1, updated NVMe configurations for different backplane adapter and risers supported.Restore eSPI maximum I/O mode for slave 0 (BMC).
7. Updated AMI 5.22_WhitleyCrb_0ACMS_ICX_070 RC27P56 for BKC 2021_WW52 (PLR1 HF).
8. Changed string "VMX" to "Intel Virtualization Technology".
9. Improved AOC-SMG3-2M2-B Marvell sensor reading.

1.1a (10/20/2021)

1. Updated 5.22_WhitleyCrb_0ACMS_ICX_069 Beta Intel BKCWW39 2021 PV MR7.
2. Updated Dx/Mx microcode from Intel-Generic-Microcode-20210927_NDA.
3. Updated SATA/sSATA EFI driver to VROC PreOS v7.6.0.1012.
4. Fixed failure of SUM Test case 254 SecureEraseDisk test.
5. Added support for SUM upload/delete HTTPS TLS certificate.
6. Changed "Hard Drive Security Frozen" default setting to disabled.

7. Applied workaround for system hang at 68 during cburn power cycle long run.
8. Fixed iPXE GPF when Redfish HI is disabled.
9. Added flag [Preserve BIOS Boot Options Configuration] controlled by BMC/SUM.
10. Modified SPS version strings and removed the "Manufacturer ID" string.
11. Disabled support for EFI iSCSI.
12. Updated SmcOOB module to 1.01.24 to support SUM clean SMBIOS Event log through BiosCfg header flag.
13. Added support for EUI-48 Locally Administered MAC Address for Redfish host interface.
14. Enhanced DMI type 42 for supporting EUI-48 Locally Administered MAC Address.
15. Updated PMaxOffset.
16. Fixed inability of NumLock item to modify by SmcPostHotKey.sd.
17. Fixed failure of SUM TC 221 when installing multiple NICs on system.
18. Fixed inability to preserve SGX settings after updating BIOS.
19. Fixed problem of the system hanging during POST when building BIOS with the token "SMC_SETUP_STYLE" as 0.
20. Fixed malfunction of Patrol Scrub on Dx ICX.
21. Corrected firmware version and vendor on Trusted Computing page.
22. Fixed inability to change COM port resource and failure of item's behavior.
23. Fixed problem of the system continuously rebooting when AOC-A25G-i2SM or AOC-A25G-M2SM is plugged in.
24. Set bits of IPMI CMD 30_A0_15 to clear according to usage of location instead of all bytes.
25. Updated eSPI maximum I/O mode for slave 0 (BMC).

1.1 (5/6/2021)

1. Set default Boot Guard profile to 5.
2. Updated Intel-Generic-Microcode.
3. Updated ASPEED VBIOS and EFI driver to 1.11.03.
4. Updated SATA/sSATA EFI driver to VROC PreOS v7.5.0.1152.
5. Kept value of setup string of Manufacturer and Product according to priority "modification of AmiBcp, FRU1, and then SMBIOS Table".
6. Added code to stop AFU support.
7. Added HCC Mx stepping CPU check for CPU stepping display.
8. Automatically disabled and hid ADDDC with x8 width DIMM.
9. Set "NVMe Firmware Source" to auto-hide when AOC-SMG3-2M2-B is plugged in.
10. Disabled MCTP for M.2 slots to prevent system hang with Micron 2300.
11. Removed 4G limit of Intel LAN memory if boot mode is not legacy.
12. Automatically disabled and grayed out ADDDC, UMA-Base Clustering, and mirror mode and enabled NUMA when SGX is enabled.
13. Enhanced SMCI HDD Security feature.
14. Extended memory DIMM serial number information (Samsung, Micron, Hynix).
15. Enhanced SMC DCPMM feature.
16. Set all OPROM control items to Legacy when boot mode is set to Dual.
17. Updated CPLD Signature table 101 and tool to 1.30.24 for CPLD Signature.
18. Updated Intel BKCWW17 2021 PV MR1.
19. Hid eADR Support item.
20. Updated SPS 4.4.4.56 PV MR2.
21. Corrected display of IPv4 address source status after updating BIOS.
22. Fixed missing SMBIOS type 17 BPS information when plugged in at P1-DIMMC2 or P2-DIMMC2.
23. Corrected location of RT UECC log.

24. Fixed failure of RT UECC to be mapped out.
25. Corrected display of IPv6 when IPv6 status is not active.
26. Filtered Dynamic HDD Security pages to patch failure of SUM ChangeBiosCfg.
27. Fixed problem of T-states always showing 15 levels even when T-state is disabled.
28. Fixed problem with a CPU exception.
29. Fixed failure to hide the SmcSecureErase setup page when no HDD devices are plugged in.
30. Corrected display of UEFI OS boot option name in BIOS setup.
31. Fixed failure of Secure Boot Append/Update Keys.
32. Fixed inability to upload all OOB files on the first BMC boot.
33. Corrected memory device number in SMBIOS type 16.
34. Corrected iSCSI Configuration page.
35. Set DIMM size to recalibrate when rank is disabled.
36. Fixed the issue of system hanging after executing sum -c EraseOAKey or afuefi /OAD.
37. Added workaround for issue of updating BIOS then rebooting causing system CPU exception at 0x79 when TXT is enabled.

1.0a (1/13/2021)

1. Updated WW51.
2. Added support for BIOS uploading/downloading OOB file to/from BMC during POST even if SMCI USB Redfish Host Interface is set to "OFF" in IPMI GUI web.
3. Fixed problem of system hanging at 0xB2 when plugging in the SATA and NVMe device.
4. Added force next boot to UEFI Shell support.
5. Implemented CPU always turbo function.
6. Added support for Linux built-in utility efibootmgr.
7. Filled Onboard LAN1 MAC address into SMBIOS Type 1 UUID field.
8. Set CMOS Battery Low event to log into SMBIOS (POST Error Type 08h).
9. Added support for changing PXE from UEFI (U)/Legacy (L) to L/U through IPMI Boot Flag Command.
10. Enabled OOB file to be uploaded/downloaded to/from BMC even if Network Stack is disabled.
11. Fixed inability of the system to boot into PXE with DVD installed.
12. Enhanced SMCI HDD Security feature.
13. Set PCLS and ADDDC to enabled by default and enabled leaky bucket of about 2.15 minutes.
14. Added Enhance PPR function.
15. Added Auto mode to "NVMe Mode Switch".
16. Added SEL for PPR success.
17. Fixed inability to find "Rear USB Port(s)" for SUM test case 343.
18. Fixed problem of system hanging at postcode "B2" when creating RAID0/1 volume.
19. Fixed problem of system exception occurring at 0x92 or 0xA2 after changing boot order and rebooting.
20. Fixed inability to correctly set some DMI data.
21. Fixed problem of system exception occurring and rebooting when using IPMI force boot to UEFI disk.
22. Fixed problem of system hanging if moving USB KB/MS when entering Windows.
23. Fixed malfunction of setup item "Maximum Read Request".
24. Corrected display of IPv6 in Early Video.
25. Fixed problem of "Configuration Address Source" always showing "DHCP" on IPMI IPv6 page.
26. Corrected Memory Correct Error location in BIOS event log for CPU2.
27. Modified IPv6 behavior to remove error message when IPv6 router IP is :::::::.
28. Corrected CPU1 memory type 20 handler point to CPU2 Memory Array Mapped Address structure.
29. Corrected display of IPv6 Status after updating BIOS.