

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	X12SPO-(NT)F
Release Version	1.2
Release Date	02/23/2022
Build Date	02/23/2022
Previous Version	1.1a
Update Category	Recommended
Dependencies	None
Important Notes	None
Enhancements	<ol style="list-style-type: none">1. Updated AMI 5.22_WhitleyCrb_0ACMS_ICX_070_BETA RC27P52 for BKC 2021_WW52 (PLR1), and RC27P56 for PLR1 HF.2. Changed string "VMX" to "Intel Virtualization Technology".3. Updated 5.22_WhitleyCrb_0ACMS_ICX_069 Beta Intel BKCWW39 2021 PV MR7, please check header for firmware revisions.4. Updated Dx/Mx microcode from Intel-Generic-Microcode-20210927_NDA.5. Extended NVMe OPRM control options to 24 slots.6. Turned on Shutdown Suppression and Log MCA IERR to fix crash dump error.7. Removed the default CA-Cert, Client-Cert, Private-Key support8. Added multiple KMS Servers Support for SmcKMS.

	<p>9. Fixed the wording of the TCG NVME KMS Policy.</p> <p>10. Changed some Setup Items types from String type to Password type.</p> <p>11. Added SmcKMS Probe function.</p> <p>12. Updated the Asp2600 module.</p> <p>13. Updated the strings on the Setup Menu relative to SmcKMS.</p> <p>14. Added more controllable items reported by SUM team. (Updated SmcKMS.efi)</p> <p>15. Enhanced PPR from Enabled to Disabled.</p> <p>16. Added item "Data Link Feature Exchange" in PCIe SLOT pages.</p>
New features	N/A
Fixes	<p>1. Removed 1G option from MMCFG base to avoid system hang.</p> <p>2. Fixed the SMBIOS event log ERROR CODE that is not displaying correctly under BIOS menu issue (EFI error type).</p> <p>3. Rolled back VROC SATA/sSATA EFI driver to VROC PreOS v7.6.0.1012 to fix system hang when VMD enable.</p> <p>4. Fixed COM port resource that can't be changed.</p> <p>5. Updated boot status to BMC at first power on for test scenario "flashing other ROM immediately".</p> <p>6. Fixed the problem reported by SUM team. (Updated SmcKMS.efi)</p> <p>7. Cleared bits of IPMI CMD 30_A0_15 according to usage of location instead of all bytes. (Built from SVN#461 in OOB)</p> <p>8. Updated SmcOutBand in SmcPKG/Module/SmcOOB to fix the problem that DMI data are not stored when executing "SUM - c LoadDefaultBiosCfg".</p>

Release Notes from Previous Release(s)

1.1a (7/30/2021)

1. Updated 5.22_WhitleyCrb_OACMS_ICX_066_BETA Intel BKCWW24 2021 PV MR4.

2. Updated Dx/Mx microcode from Intel-Generic-Microcode-20210701_NDA.
3. Updated SATA/sATA EFI driver to VROC PreOS v7.6.0.1012.
4. Updated SPS 4.4.4.56 PV MR2.
5. Fixed the issue with TPM 1.2/2.0 disappearing when enabling Intel "TXT Support" without provisioning Intel TXT requiring NV indices to TPM.
6. Changed "Hard Drive Security Frozen" default setting to disabled.
7. Added support to SUM upload/delete HTTPS TLS certificate. (Default disabled by TOKEN "Sum_UploadTlsKey_SUPPORT")
8. Disabled EFI iSCSI support.
9. Path BMC Redfish Host Interface was renamed as ethX for the case where CDN was disabled under Linux OS.
10. Fixed the issue that WHLK TPM 2.0 Supplemental test failed.
11. Fixed the issue with SGX settings not getting preserved after updating BIOS. The function cannot support IPMI web updating BIOS.
12. Fixed the issue due to which wrong FW version and vendor were shown on Trusted computing page.

1.1 (4/9/2021)

1. Updated RC 20.P95 for PV RC update.
2. Updated SPS 4.4.4.53.
3. Updated Intel-Generic-Microcode-20210226a_NDA and Intel AE.
4. Corrected BIOS version that shows in IPMI after ROT recovery of previous version of BIOS.
5. Added support for VROC OOB.
6. Removed iSCSI option from LAN OPROM item.
7. Set PCH PCIe ASPM to disabled if CPU PCIe global ASPM is disabled.
8. Changed "SMCI PMem Formset" to "SMCI PMem Configuration".
9. Corrected memory device number in SMBIOS type 16.
10. Fixed problem with a CPU exception.
11. Fixed problem of T-states always showing 15 levels even when T-state is disabled.

1.0a (3/5/2021)

1. Updated VBIOS and VGA EFI driver to 1.11.03.
2. Updated 5.22_WhitleyCrb_OACMS_ICX_058_BETA for PC2 RC update.
3. Updated BIOS ACM 1.0.9 and SINIT ACM 1.0.9.
4. Updated SPS 4.4.51.
5. Updated Firmtool 1.30.21 to 1.30.22.
6. Updated SATA/sATA EFI driver to VROC PreOS v7.5.0.1152.
7. Added PROMPT_F1_ON_PWD_TRYOUT.
8. Added IPMI OEM command 0x30 0x68 0xE0 to enhance SUM OOB flow.
9. Kept value of setup string of Manufacturer and Product according to priority "modification of AmiBcp, FUR1, and then SMBIOS Table".
10. Fixed inability of the system to boot into PXE with DVD installed.
11. Enhanced SMCI HDD Security feature.
12. Added the new type "text" of the HII data for the SMC setup modify function.
13. Set GPP_C20 to GPIO default output high to prevent PCH throttle.
14. Added support for recovering boot status after flashing ROM through BMC/CPLD.
15. Added code to stop AFU support.
16. Added HCC Mx stepping CPU check for CPU stepping display.

17. Set default Boot Guard profile to 5.
18. Extended memory DIMM serial number information (Samsung, Micron, Hynix).
19. Enhanced SMC DCPMM feature.
20. Automatically disabled and hid ADDDC with x8 width DIMM.
21. Provided Redfish BootOptions with complete DevicePath information.
22. Removed 4G limit of Intel LAN memory if boot mode is not legacy.
23. Updated OOB Module to 1.01.22.
24. Set relation setup to restore setting after "Factory Mode" is disabled.
25. Exported AVX P1 (Config TDP) item.
26. Automatically disabled and grayed out ADDDC, UMA-Base Clustering, and mirror mode and enabled NUMA when SGX is enabled.
27. Set all OPRON control items to Legacy when boot mode is set to Dual.
28. Set PROCHOT Modes to Input-Only.
29. Fine tuned BMC LAN USB error handle and fixed asset problem when enabling BIOS debug mode and rebooting BMC under UEFI shell.
30. Fixed failure of the HDD security menu to show when more than 6 HDDs are connected on system.
31. Fixed failure of the BIOS binary to follow the unique format on the PC with Python 3 installed.
32. Fixed failure of SUT to prompt "Enter User password" screen after setting a password when plugging in SED device.
33. Corrected display of IPv4 address source status after updating BIOS.
34. Corrected display of IPv6 status after updating BIOS.
35. Modified IPv6 behavior and removed error message when IPv6 router IP is ::::.
36. Fixed problem of "Configuration Address Source" always showing "DHCP" on IPMI IPv6 page.
37. Fixed problem of BIOS initialization showing IPV6 address when IPV6 is disabled in the IPMI GUI.
38. Prevented failure of Redfish check items using items with same SGX_PROMPT Name and different offset.
39. Fixed malfunction of AFU /n.
40. Filtered Dynamic HDD Security pages to patch failure of SUM ChangeBiosCfg.
41. Set AFU to stop if there are no parameters.
42. Fixed problem of module recovering boot status again when CMOS is clear.
43. Corrected location of RT UECC log.
44. Fixed failure of RT UECC to be mapped out.
45. Adjusted InBand RomHole size to prevent insufficient InBand Update Bios Cfg buffer size.
46. Corrected display of UEFI OS boot option name in BIOS setup.
47. Fixed failure of Secure Boot Append/Update Keys.
48. Fixed inability to upload all OOB files on the first BMC boot.
49. Corrected display of IPv6 when IPv6 status is not active.
50. Fixed mismatch of memory device in IPMI and in BIOS setup when some memory DIMMs are mapped out.
51. Corrected LAN MAC in IPMI web.