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	**X12SPL-(LN4)F**
Release Version	**1.4**
Release Date	**07/14/2022**
Build Date	**07/14/2022**
Previous Version	**1.2**
Update Category	**Recommended**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Update Intel BKCWW23 PLR3 for INTEL-SA-00657 and INTEL-SA-00686 security issues** **2. Updated VROC SATA/sSATA EFI driver to VROC PreOS v7.7.6.1004 to adress INTEL-TA-00692.** **3. Added "CSM Support" setup item into SMCISBForm page.** **4. Updated ucode M87606A6_0D000375 to address CVE-2022-21233 and CVE-2021-33060.** **5. Added Link Retrain per port in BIOS.**
New features	**N/A**
Fixes	**1. Fixed SATA device, functioning abnormally.** **2. If chassis type of FRU0 is not 1(other) or 2(unknown), sync it to SMBIOS type 3.**

Release Notes from Previous Release(s)

1.2 (5/3/2022)

1.Update BIOS version to 1.2.
2.Update AMI 5.22_WhitleyCrb_0ACMS_ICX_070_BETA RC27P52 for BKC 2021_WW52 (PLR1), and RC27P56 for PLR1 HF.
3.Changed string "VMX" to "Intel Virtualization Technology".
4.Removed 1G option from MMCFG base to avoid system hang.
5.Fixed the SMBIOS event log ERROR CODE not display correctly under BIOS menu issue (EFI error type).
6.Rolled back VROC SATA/sSATA EFI driver to VROC PreOS v7.6.0.1012 to fix system hang when VMD is enabled.
7.Fixed issue with password that can't be preserved after loading default via Supermicro Update Manager (SUM).

1.1c (11/15/2021)

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. Extended NVMe OPROM control options to 24 slots.
4. Turned on Shutdown Suppression and Log MCA IERR to fix crash dump error.
5. Removed support for the default CA-Cert, Client-Cert, and Private-Key.
6. Added multiple KMS Server Support for SmcKMS.
7. Fixed the wording of the TCG NVMe KMS Policy.
8. Changed some Setup Item types from String type to Password type.
9. Added SmcKMS Probe function.
10. Updated Asp2600 module.
11. Updated the strings on the Setup Menu related to SmcKMS.
12. Added "DelCaCert", "DelClientCert", and "DelClientPriKey" into SmcOOB Interface for SUM to remove CERT keys.
13. Set Enhanced PPR from Enabled to Disabled.
14. Displayed item "Data Link Feature Exchange" on PCIe SLOT pages.
15. Fixed inability to change COM port resource and failure of item's behavior.
16. Updated boot status to BMC at first power-on for test scenario "flashing other ROM immediately".
17. Removed 1G option from MMCFG base to prevent system hang.
18. Fixed problem of only one CERT key updating successfully when updating all CERT keys (CA, Client Cert, and Private Key) by BIOSCfg at the same time.
19. Implemented restoration of ROM-Hole and NVRAM Variables that should be kept after checking if GUID-HOB (NvramLoadDefaultModeGuid) exists.
20. Set bits of IPMI CMD 30_A0_15 to be cleared according to usage of location instead of all bytes.
21. Updated SmcOutBand in SmcPKG/Module/SmcOOB to fix the failure to store DMI data when executing "SUM -c LoadDefaultBiosCfg".

1.1a (07/30/2021)

1. Updated 5.22_WhitleyCrb_0ACMS_ICX_066_BETA Intel BKCWW24 2021 PV MR4.
2. Updated Dx/Mx microcode from Intel-Generic-Microcode-20210701_NDA.
3. Updated SATA/sSATA 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 BIOS ACM 1.0.9 and SINIT ACM 1.0.9.
3. Updated SPS 4.4.4.53.
4. Automatically disabled and hid ADDDC with x8 width DIMM.
5. Extended memory DIMM serial number information (Samsung, Micron, Hynix).
6. Enhanced SMC DCPMM feature.
7. Automatically disabled and grayed out ADDDC, UMA-Base Clustering, and mirror mode and enabled NUMA when SGX is enabled.
8. Set relation setup to restore setting after "Factory Mode" is disabled.
9. Removed 4G limit of Intel LAN memory if boot mode is not legacy.
10. Set all OPROM control items to Legacy when boot mode is set to Dual.
11. Updated SATA/sSATA EFI driver to VROC PreOS v7.5.0.1152.
12. Updated BPS firmware to 2.2.0.1553.
13. Set BootGuard to enabled by default.
14. Removed iSCSI option from LAN OPROM item.
15. Removed 4G limit of Intel LAN memory if boot mode is EFI.
16. Set PCH PCIe ASPM to disabled if CPU PCIe global ASPM is disabled.
17. Stopped sending major code 0x2A (no memory) SEL.
18. Added support for VROC OOB.
19. Changed "SMCI PMem Formset" to "SMCI PMem Configuration".
20. Fixed problem of BIOS initialization showing IPV6 address when IPV6 is disabled in the IPMI GUI.
21. Filtered Dynamic HDD Security pages to patch failure of SUM ChangeBiosCfg.
22. Set AFU to stop if there are no parameters.
23. Fixed mismatch of memory device in IPMI and in BIOS setup when some memory DIMMs are mapped out.
24. Corrected display of IPv6 when IPv6 status is not active.
25. Fixed inability to upload all OOB files on the first BMC boot.
26. Fixed failure of Secure Boot Append/Update Keys.
27. Corrected display of UEFI OS boot option name in BIOS setup.
28. Corrected SMBIOS Type 41 onboard VGA description string to AST2600.
29. Fixed failure of SUT to prompt "Enter User password" screen after setting a password when plugging in SED device.
30. Fixed failure of the HDD security menu to show when more than 6 HDDs are connected on system.
31. Fixed inability of AOC NVMe card to change to VMD mode when setting NVMe switch to VMD.

32. Fixed inability to report onboard LAN MAC address to IPMI when onboard LAN uses 64bit memory resource.
33. Fixed failure of Microsoft HLK certification and TPM 2.0 UEFI Preboot Interface Test on Microsoft Server 2019.
34. Fixed problem with a CPU exception.
35. Fixed failure to hide the SmcSecureErase setup page when no HDD devices are plugged in.
36. Fixed problem of T-states always showing 15 levels even when T-state is disabled.
37. Recalibrated DIMM size when rank is disabled.
38. Corrected memory device number in SMBIOS type 16.