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.

Product Name	**X12SPi-TF**
Release Version	**1.1c**
Release Date	**11/8/2021**
Build Date	**11/8/2021**
Previous Version	**1.0**
Update Category	**Recommended**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Updated 5.22_WhitleyCrb_0ACMS_ICX_069 Beta Intel BKCWW39 2021 PV MR7.** **2. Updated M87606A6_0D000311 microcode for Dx/Mx stepping CPU for Intel-TA-00586: CVE-2021-33117 (Medium 6.5)** **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 the default CA-Cert, Client-Cert, Private-Key support.** **6. Added multiple KMS Servers Support for SmcKMS.**
New features	**N/A**
Fixes	**1. Fixed inability to change COM port resource and item's behavior.** **2. Cleared IPMI CMD 30_A0_15 bits according to usage of location instead of all bytes.** **3. Removed 1G option from MMCFG base to avoid system hanging.**

	4. Updated boot status to BMC at first power on for test scenario "flashing other ROM immediately". **5. Fixed the SMBIOS event log ERROR CODE not displaying correctly under BIOS menu issue (EFI error type).**

Release Notes from Previous Release(s)

1.1a (7/30/2021)

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 SPS 4.4.4.53.
3. Updated Intel-Generic-Microcode-20210402_NDA and Intel AE.
4. Enabled the ability to check when the onboard LAN connection drops.
5. Fixed the wrong BIOS version showing IPMI after ROT recovery.
6. Added VROC OOB support.
7. Fixed a CPU exception that occurs when changing BIOS config with SUM.
8. Fixed T-states always showing 15 levels even when T-state is disabled.

1.0a (3/5/2021)

1. Updated 5.22_WhitleyCrb_0ACMS_ICX_058_BETA for PC2 RC update.
2. Updated BIOS ACM 1.0.9 and SINIT ACM 1.0.9.
3. Updated SPS 4.4.51.
4. Fixed inability of the system to boot into PXE with DVD installed.
5. Kept setup string of BiosVersion, BiosDate, Manufacturer, and Product as default value including modification of AmiBcp.
6. Kept value of setup string of Manufacturer and Product according to priority "modification of AmiBcp, FUR1, and then SMBIOS Table".
7. Updated Intel-Generic-Microcode-20210226a_NDA and Intel AE.
8. Automatically disabled and hid ADDDC with x8 width DIMM.
9. Extended memory DIMM serial number information (Samsung, Micron, Hynix).
10. Enhanced SMC DCPMM feature.
11. Automatically disabled and grayed out ADDDC, UMA-Base Clustering, and mirror mode and enabled NUMA when SGX is enabled.
12. Set relation setup to restore setting after "Factory Mode" is disabled.
13. Removed 4G limit of Intel LAN memory if boot mode is not legacy.
14. Set all OPROM control items to Legacy when boot mode is set to Dual.
15. Updated SATA/sSATA EFI driver to VROC PreOS v7.5.0.1152.
16. Updated BPS firmware to 2.2.0.1553.
17. Set BootGuard to enabled by default.
18. Fixed problem of "Configuration Address Source" always showing "DHCP" on IPMI IPv6 page.

19. Modified IPv6 behavior and removed error message when IPv6 router IP is ::::::.

20. Corrected display of IPv6 status after updating BIOS.

21. Corrected display of IPv4 address source status after updating BIOS.

22. Prevented failure of Redfish check items using items with same SGX_PROMPT Name and different offset.

23. Fixed problem of BIOS initialization showing IPV6 address when IPV6 is disabled in the IPMI GUI.

24. Filtered Dynamic HDD Security pages to patch failure of SUM ChangeBiosCfg.

25. Set AFU to stop if there are no parameters.

26. Fixed mismatch of memory device in IPMI and in BIOS setup when some memory DIMMs are mapped out.

27. Corrected display of IPv6 when IPv6 status is not active.

28. Fixed inability to upload all OOB files on the first BMC boot.

29. Fixed failure of Secure Boot Append/Update Keys.

30. Corrected display of UEFI OS boot option name in BIOS setup.

31. Corrected SMBIOS Type 41 onboard VGA description string to AST2600.