BIOS Release Notes Form

Product Name	**X12SPM-TF/LN4F/LN6T**
Release Version	**1.1c SPS 4.4.4.58**
Release Date	**11/12/2021**
Build Date	**11/12/2021**
Previous Version	**1.1b**
Update Category	**Critical**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Updated BIOS version to 1.1c.** **2. Updated 5.22_WhitleyCrb_0ACMS_ICX_069 Beta Intel BKCWW39 2021 PV MR7.** **3. Updated Dx/Mx microcode from Intel-Generic-Microcode-20210927_NDA.** **4. Updated BIOS ACM to 20210720 (1.0.D) and SINIT ACM 20210827 (1.0.F).** **5. Updated SPS 4.4.4.58.** **6. Exposed the "Data Link Feature Exchange" BIOS setting in PCIe SLOT pages.**
New features	**N/A**
Fixes	**1. Removed the 1G option from MMCFG base to avoid system hang.**

	2. Updated BMC boot status to indicate that the ROM is being flashed at a different memory location. **3. Enabled changing PCIe lane from x8 to x16 when an AOC is inserted in slot 1 of RSC-H2-68G4.** **4. Updated SmcOutBand in SmcPKG/Module/SmcOOB to allow the DMI data to be stored when executing "SUM -c LoadDefaultBiosCfg".**

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 (4/29/2021)

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. Updated SATA/sSATA EFI driver to VROC PreOS v7.5.0.1152.
5. Set all OPROM control items to Legacy when boot mode is set to Dual.
6. Removed iSCSI option from LAN OPROM item.
7. Fixed malfunction of ONBORAD_LAN_DROP_CHECK under some conditions.

1.0a (3/5/2021)

1. Updated VBIOS and VGA EFI driver to 1.11.03.
2. Updated BIOS ACM 1.0.9 and SINIT ACM 1.0.9.

3. Updated 5.22_WhitleyCrb_0ACMS_ICX_058_BETA for PC2 RC update.
4. Enhanced SmcSecureBoot function.
5. Updated Firmtool 1.30.21 to 1.30.22.
6. Updated SATA/sSATA EFI driver to VROC PreOS v7.5.0.1152.
7. Updated BPS firmware 1553 and UEFI driver 3852.
8. Added PROMPT_F1_ON_PWD_TRYOUT.
9. Added IPMI OEM command 0x30 0x68 0xE0 to enhance SUM OOB flow.
10. Kept value of setup string of Manufacturer and Product according to priority "modification of AmiBcp, FUR1 and then SMBIOS Table".
11. Fixed inability of the system to boot into PXE with DVD installed.
12. Enhanced SMCI HDD Security feature.
13. Added the new type "text" of the HII data for the SMC setup modify function.
14. Set GPP_C20 to GPIO default output high to prevent PCH throttle.
15. Added support for recovering boot status after flashing ROM through BMC/CPLD.
16. Added code to stop AFU support.
17. Added HCC Mx stepping CPU check for CPU stepping display.
18. Set default Boot Guard profile to 5.
19. Updated AMI 5.21_WhitleyCrb_0ACMS_ICX_056 for PC2 RC update.
20. Automatically disabled and hid ADDDC with x8 width DIMM.
21. Extended memory DIMM serial number information (Samsung, Micron, Hynix).
22. Updated Intel-Generic-Microcode-20210226a_NDA and Intel AE.
23. Updated SPS 4.4.51.
24. Fine tuned BMC LAN USB error handle and fixed asset problem when enabling BIOS debug mode and rebooting BMC under UEFI shell.
25. Fixed failure of the HDD security menu to show when more than 6 HDDs are connected on system.
26. Fixed failure of the BIOS binary to follow the unique format on the PC with Python 3 installed.
27. Fixed failure of SUT to prompt "Enter User password" screen after setting a password when plugging in SED device.
28. Corrected display of IPv4 address source status after updating BIOS.
29. Corrected display of IPv6 status after updating BIOS.
30. Modified IPv6 behavior and removed error message when IPv6 router IP is :::::::.
31. Fixed problem of "Configuration Address Source" always showing "DHCP" on IPMI IPv6 page.
32. Fixed system auto reboot when AOC-S100G-b2C is in slot 7.
33. Fixed malfunction of EDPC.
34. Set AFU to stop if there are no parameters.
34. Fixed problem of module recovering boot status again when CMOS is clear.