BIOS Release Notes Form

Product Name	**X12SPM-TF/LN4F/LN6T**
Release Version	**1.6**
Release Date	**08/28/2023**
Build Date	**08/28/2023**
Previous Version	**1.5**
Update Category	**Recommended**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Updated BIOS version to 1.6.** **2. Updated 5.22_WhitleyCrb_0ACMS_ICX_076_BETA (IPU-PV 2023.3) for INTEL-SA-00813 Security Advisory to address CVE-2022-37343 (7.2, High), CVE-2022-44611 (6.9, Medium), CVE-2022-38083 (6.1, Medium), CVE-2022-27879 (5.3, Medium) and CVE-2022-43505 (4.1, Medium) security issues; and for INTEL-SA-00837 Security Advisory to address CVE-2022-41804 (7.2, High) security issue.** **3. Enhanced the BMC/BMC Network Configuration page IPv6 DNS/DNS2 setting.** **4. Changed strings from "Lock mode" to "Lockdown mode".** **5. Updated Intel Server Platform Services for Whitley Server Platforms IPU2023.3 4.4.4.500 for INTEL-SA-00813 Security Advisory to address CVE-2022-37343 (7.2, High), CVE-2022-44611 (6.9, Medium), CVE-2022-38083 (6.1, Medium), CVE-2022-27879 (5.3, Medium) and CVE-2022-43505 (4.1, Medium) security issues; and for INTEL-SA-00837 Security Advisory to address CVE-2022-41804 (7.2, High) security issue.** **6. Updated M87606A6_0D0003A5 microcode for Dx stepping CPU for INTEL-SA-00813 Security Advisory to address CVE-**

	2022-37343 (7.2, High), CVE-2022-44611 (6.9, Medium), CVE-2022-38083 (6.1, Medium), CVE-2022-27879 (5.3, Medium), and CVE-2022-43505 (4.1, Medium) security issues; for INTEL-SA-00828 Security Advisory to address CVE-2022-40982 (6.5, Medium) security issue; for INTEL-SA-00836 Security Advisory to address CVE-2023-23908 (6.5, Medium) security issue; and for INTEL-SA-00837 Security Advisory to address CVE-2022-41804 (7.2, High) security issue.
New features	**N/A**
Fixes	**1. Fixed the issue that SMBIOS Type0 System Family change could not be preserved after clearing CMOS.** **2. Fixed ENERGY_PERF_BIAS_CFG Mode item changing to default after SUM update BIOS with the "--preserve_setting" command.**

Release Notes from Previous Release(s)

1.5 (04/18/2023)

1. *Updated BIOS version to 1.5.*
2. *Update 5.22_WhitleyCrb_0ACMS_ICX_075 Intel 2023.2 IPU-PV, please check header for firmware revisions.*
3. *Updated Intel Server Platform Services for Whitley Server Platforms IPU2023.1 4.4.4.301.*
4. *Fixed an issue where memory errors were not being reported in the SMBIOS event log.*

1.4a (12/13/2022)

1. *Updated BIOS version to 1.4a.*
2. *Updated 5.22_WhitleyCrb_0ACMS_ICX_73 Intel BKCWW40 PLR3 OOB. Please check the header for firmware revisions.*
3. *Updated M87606A6_0D00037B microcode for Dx/Mx stepping CPU.*
4. *Updated the VROC SATA/sSATA EFI driver to VROC PreOS v7.8.0.1012 to address Intel Virtual RAID on CPU (VROC): Data Loss Exposure Due to RAID 5 TRIM Support document #737276.*
5. *Updated the DBX file to fix Secure Boot Bypass issue.*
6. *Followed the SMBIOS template sync the chassis type from FRU0 to SMBIOS Type 03. Removed ignore sync up SMBIOS Type 03 when the chassis type is unknown or other.*
7. *Corrected gPayloadOffset definition to fix the inability to successfully program NVRAM with the AFU utility.*

1.4 (7/12/2022)

1. *Updated BIOS version to 1.4.*
2. *Updated 5.22_WhitleyCrb_0ACMS_ICX_72 Intel BKCWW23 PLR3, please check header for firmware revisions. For INTEL-SA-00657 Security Advisory to address CVE-2022-21233(6.0, Medium) security issue. For INTEL-SA-00686 Security Advisory to address CVE-2021-33060(7.8, High) security issue.*
3. *Updated VROC SATA/sSATA EFI driver to VROC PreOS v7.7.6.1004 to adress INTEL-TA-00692. CVE-2022-29919(7.8 High), CVE-2022-30338(6.7 Medium), CVE-2022-29508(6.3 Medium), CVE-2022-25976(5.5 Medium) Update VROC SATA/sSATA legacy driver to VROC PreOS v6.3.5.1003 Hot Fix to fix 10TB or higher volume drive issue.*
4. *Added "CSM Support" setup item into SMCISBForm page.*
5. *Updated ucode M87606A6_0D000375 to address below issue. For INTEL-SA-00657 Security Advisory to address CVE-2022-21233(6.0, Medium) security issue. For INTEL-SA-00686 Security Advisory to address CVE-2021-33060(7.8, High) security issue.*
6. *If chassis type of FRU0 is not 1(other) or 2(unknown), sync it to SMBIOS type 3. Disabled Link Re-train in BIOS to avoid secondary Bus Reset following intel MOW 22WW27 and expose Link Re-train per port in BIOS.*

1.2 (2/18/2022)

1. Updated BIOS version to 1.2.
2. Updated 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".
N/A
3. Rolled back VROC SATA/sSATA EFI driver to VROC PreOS v7.6.0.1012 to fix system hang when VMD is enabled.
4. Removed 1G option from MMCFG base to avoid system hang.
5. Fixed the SMBIOS event log ERROR CODE not displaying correctly under BIOS menu issue (EFI error type).

1.1c (11/12/2021)

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.
7. Removed the 1G option from MMCFG base to avoid system hang.
8. Updated BMC boot status to indicate that the ROM is being flashed at a different memory location.
9. Enabled changing PCIe lane from x8 to x16 when an AOC is inserted in slot 1 of RSC-H2-68G4.
10. Updated SmcOutBand in SmcPKG/Module/SmcOOB to allow the DMI data to be stored when executing "SUM -c LoadDefaultBiosCfg".

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.