BIOS Release Notes Form

Product Name	**X11SCW-F**
Release Version	**2.1**
Release Date	**7/5/2023**
Build Date	**7/5/2023**
Previous Version	**2.0**
Update Category	**Recommended**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Updated Microcode 906EA to 0xf4 and 906ED to 0xfa per IPU 2023.3 Processor Advisory INTEL-TA-00828 to address CVE-2022-40982 (6.5 Medium).** **2. Updated SPS_E3_05.01.04.913.0 and RC per IPU 2023.3 Processor Advisory.** **3. Updated RC per IPU 2023.3 Processor Advisory.**
New features	**None**
Fixes	**1. Ported code for supporting ofid check.** **2. Corrected SUM_BIOS_OEM_FID_SUPPORT configure to SMC_OEMFID_SUPPORT.**

Release Notes from Previous Release(s)

2.0 (2/18/2023)

1. *Changed BIOS version to 2.0.*
2. *Modified Smbios eModule for security update for AMI advisory SA50090.*
3. *Modified CmosManager, ACHI, FlashSmi, HddSecurity, NVME, NVRAM, LegacySerialRedirection, OemActivation, Recovery, SecureFlash, TcgStorageSecurity, Smbios for security update for AMI advisory SA50121 to address CVE-2021-33164 (7.5 High).*
4. *Modified SmmSmbiosElogInitFuncs.c for security update for AMI advisory SA50127.*
5. *Update Reference Code for Intel 2023.1 IPU for INTEL-TA-00717 to address CVE-2022-26837 (7.5 High) and CVE-2022-33894 (7.5 High).*
6. *Updated SPS FW to SPS_E3_05.01.04.804 for IPU 2023.1.*
7. *Enabled Flash SMI support.*

1.9 (9/21/2022)

1. *Updated Uefi Network Stack to label 28 and added patch for AMI SA-50110 security issue.*
2. *According to new rule, changed setup string "SMCI" to "Supermicro."*
3. *Updated DBX revocation packages released on UEFI.org on 08/15/2022 to fix Secure Boot Bypass issue.*
4. *Integration for IPU 2022.3 Reference Code IPU PV.*
5. *Updated SPS FW to SPS_E3_05.01.04.700.0 for IPU 2022.3.*
6. *Changed BIOS version to 1.9.*
7. *Updated 906ED Microcode to 0xF4 for IPU 2022.3.*
8. *Fixed resign fail when request sign.*

1.8 (5/13/2022)

1. *Changed BIOS version to 1.8.*
2. *Synced up 5.13_1AURF_RC7.0.58.50_054(189.B09).*
3. *Updated Microcode M22906EA_000000F0(U-0 Stepping) and M22906ED_000000F0(R-0 Stepping) for Intel 2022.1 IPU.*
4. *Updated Intel SINIT ACM to 1.10.1 for Intel 2022.1 IPU.*
5. *Updated SPS FW to SPS_E3_05.01.04.600.0 for IPU 2022.2.*

Fixed the following issues:

6. *When using SMC IPMITool IPMI power boot option 14(UEFI PXE), the system should scan all LAN ports for UEFI PXE boot.*
7. *Updated Uefi Network Stack to label 28 and add patch for AMI SA-50110 security issue.*
8. *Fixed automation test case "Check Https Boot" fail.*

1.7a (3/9/2022)

Changed BIOS version to 1.7a.
Added Force Next Boot feature to UEFI Shell support, to boot to UEFI automatically.

1.7 (01/19/2022)

1. Changed BIOS version to 1.7.

2. Updated Intel SINIT ACM to 1.9.1. For INTEL-TA-00527 to address CVE-2021-0107 (7.2 High), CVE-2021-0111 (7.2 High), CVE-2021-0114 (7.9 High), CVE-2021-0115 (7.9 High), CVE-2021-0116 (7.9 High), CVE-2021-0117 (7.9 High) and CVE-2021-0118 (7.9 High) security issues.
3. Fixed CATERR - Assertion when using Intel X722-DA2.
4. Update Microcode M22906EA_000000EC(U-0 Stepping), M02906EB_000000EC(B-0 Stepping), M22906EC_000000EC(P-0 Stepping) and M22906ED_000000EC(R-0 Stepping) for INTEL-TA-00532 . Security Advisory to address CVE-2021-0127 (5.6 Medium) security issue.
5. Updated SPS FW to SPS_E3_05.01.04.400 for INTEL-TA-00470 Security Advisory to address CVE-2021-0060 (7.3 High) IPU 2021.2.
6. Update RC to Mehlow Refresh version 7.0.58.50 for INTEL-TA-00527 Security Advisory to address CVE-2021-0092 (4.7 Medium) and CVE-2021-0156 (7.5 High), INTEL-TA-00562 Security Advisory to address CVE-2021-0157 (8.2 High) security issue.
7. Fixed the UEFI boot order, it does not follow the BIOS template.
8. Fix SUM cannot get the item "Software Guard Extensions (SGX)" of BIOS configuration via sum -c getcurrentbioscfg command.

1.6 (05/28/2021)

1. Changed the BIOS version to 1.6.
2. Fixed CATERR – Assertion event when using Intel X722-DA2.
3. Updated microcodes M22906EA_000000EA(U-0 Stepping) for Intel 20211IPU for INTEL-SA-00464 Security Advisory to address CVE-2020-24512 (2.8, Low) security issue.
4. Updated SPS FW to SPS_E3_05.01.04.303 for Intel 20211IPU for INTEL-TA-00459 Security Advisory to address CVE-2020-24509 (6.7, Medium) security issue.
5. Update Intel BIOS ACM & SINIT ACM to 1.8.0 for Intel 20211IPU for INTEL-TA-00463 to address CVE-2020-12357 (7.5 High), CVE-2020-8670 (7.5 High), and CVE-2020-12360 (5.6 Medium) security issues.

1.5a (03/23/2021)

1. Changed the BIOS version to 1.5a.
2. Updated SPS firmware to SPS_E3_05.01.04.300.0 for IPU 2021.1 for INTEL-SA-00459 Security Advisory to address CVE-2020-24509 (6.7, Medium), CVE-2020-8704 (6.7, Medium), CVE-2020-24507 (6.0, Medium), CVE-2020-8703 (5.1, Medium), and CVE-2020-24506 (4.4, Medium) security issues.
3. Copied the BIOS binary and renamed it to meet the unique name format.
4. Updated microcodes M02906EB_000000EA (B-0 Stepping), M22906EC_000000EA (P-0 Stepping), and M22906ED_000000EA (R-0 Stepping) for Intel 20211IPU for INTEL-SA-00464 Security Advisory to address CVE-2020-24511 (5.6, Medium) and CVE-2020-24512 (2.8, Low) security issues.
5. Set the ME power on sequence tPCH46 and tPCH45.
6. Fixed failure of SUM test 220 due to "PCI AER Support" and "Memory Corrected Error Enabling" setting failing to preserve after flashing BIOS.

1.5 (10/12/2020)

1. Added inband flash status event log to IPMI MEL.
2. Added Hotkey Message Enable/Disable function.
3. Updated SPS firmware to SPS_E3_05.01.04.208.0 for INTEL-TA-00391 Security Advisory to address CVE-2020-8744 (7.2, High) and CVE-2020-8755 (4.6, Medium) security issues.

4. Updated microcodes M22906EA_000000DE (U-0 Stepping), M02906EB_000000DD_000000DE (B-0 Stepping), M22906EC_000000DE (P-0 Stepping), and M22906ED_000000DE (R-0 Stepping) for Intel IPU 2020.2.
5. Updated Intel IPU 2020.2 RC 7.0.58.47 for Mehlow Refresh Server Platform Service Version.
6. Changed the BIOS version to 1.5.
7. Enhanced SMCI HDD Security feature.
8. Removed the FWSTS SMBIOS table.
9. Updated CmosManager_09 and SecureFlash_23 for AMI-SA50081 Security Update.
10. Reduced Rowhammer susceptibility for AMI-SA50084 DDR4 Rowhammer vulnerability to address CVE-2020-10255 (9.0, high) security issue.
11. Added use of Intrusion SMI to notify BMC the system has chassis intrusion.
12. Fixed problem of BIOS setup menu showing "Unknown" when plugging in the InnoDisk memory and boot up into BIOS setup menu.

1.4 (5/26/2020)

1. Changed the BIOS version to 1.4.
2. Implemented IPU 2020.1 update to SPS firmware to SPS_E3_05.01.04.113.0.
3. Enhanced the OEM FID feature to support UUID.
4. Updated Intel RSTe RAID Option ROM/UEFI Driver to 6.3.0.1005.
5. Added SMCI HDD Security feature.
6. Updated microcodes M22906EA_000000D6 (U-0 Stepping), M02906EB_000000D6 (B-0 Stepping), M22906EC_000000D6 (P-0 Stepping), and M22906ED_000000D6 (R-0 Stepping) for INTEL-SA-00320 Security Advisory to address CVE-2020-0543 (6.5, High) security issue, and microcodes M22906EA_000000D6 (U-0 Stepping), M02906EB_000000D6 (B-0 Stepping), M22906EC_000000D6 (P-0 Stepping), and M22906ED_000000D6 (R-0 Stepping) for INTEL-SA-00329 Security Advisory to address CVE-2020-0548 (2.8, Low) and CVE-2020-0549 (6.5, Medium) security issues.
7. Set the OverclockingLock flag to enabled by default for SGX test.
8. Added support for InnoDisk memory.
9. Added use of BIOS setup menu to enable/disable LAN1/LAN2 feature.
10. Fixed inability to change the serial port IO resource.
11. Fixed failure of Secure Erase password and problem of BIOS returning "EFI_Device_Error" with SED: Seagate ST1000NX0353.

1.3 (2/20/2020)

1. Changed the BIOS version to 1.3.
2. Updated BiosAcm to 1.7.1 (20191213) and SinitAcm to 1.7.8 (20191220) for INTEL-SA-00240 to address CVE-2019-0151 (7.5, High) and CVE-2019-0152 (8.2, High), for INTEL-SA-00220 to address CVE-2018-0123 (8.2, High) and CVE-2019-0124 (8.2, High), and INTEL-SA-00164 to address CVE-2019-0184 (6.0, Medium).
3. Added solution for problem of systems with LPDDR3 2133 MT/s DRAMs failing during boot.
4. Corrected the "DeepSx Power Policies" item string.
5. Updated RC to Mehlow Refresh PV version 7.0.58.44.
6. Displayed the "SGX Launch Control Policy" items in the BIOS setup menu.
7. Added SMC HDD Security feature.
8. Updated Microcodes M22906EA_000000D2 (U-0 Stepping), M02906EB_000000D2 (B-0 Stepping), M22906EC_000000D2 (P-0 Stepping), and M22906ED_000000D2 (R-0 Stepping) for INTEL-SA-00320

Security Advisory to address CVE-2020-0543 (6.5, High) security issue and for INTEL-SA-00329 Security Advisory to address CVE-2020-0548 (2.8, Low) and CVE-2020-0549 (6.5, Medium) security issue.
9. Updated flag for skipping password prompt window.
10. Fixed inability of BIOS to load default when plugging in M.2.
11. Added support for erasing NVMe Opal device (like Samsung 970 EVO model MZ-V7E250) without setting admin password.

1.2 (10/24/2019)

1. Changed BIOS version to 1.2.
2. Added support for BMC AUX revision displaying.
3. Disabled the MCTP for buggy BMC workaround.
4. Updated Microcode M22906EA_000000C6 (U-0 Stepping), M02906EB_000000C6 (B-0 Stepping), Microcode M22906EC_000000C6 (P-0 Stepping), and M22906ED_000000C6 (R-0 Stepping) for INTEL-SA-00270 Security Advisory to address CVE-2019-11135 (6.5, Medium) security issue.
5. Updated the SINIT ACM to version 1.7.3 for INTEL-SA-00220 Security Advisory to address CVE-2018-0123 (8.2, High) and CVE-2019-0124 (8.2, High) security issues.
6. Updated SPS firmware to SPS_E3_05.01.03.094.0.
7. Updated the Intel PMC firmware to 300.2.11.1022.
8. Updated the AMI TSE to 2.20.1276.
9. Updated RC to Mehlow Refresh PV version 7.0.58.43 for INTEL-SA-00260 Security Advisory to address CVE-2019-0154 (6.5, Medium) security issue.
10. Updated NVRAM NVMe HddSecurity SmmConfidentialMemModule and TcgStorageSecurity to INTEL-SA-00254 request version for INTEL-SA-00254 Security Advisory to address CVE-2019-0185 (6.0, Medium) security issue.

1.0b (5/16/2019)

1. Added support for Linux built-in utility efibootmgr.
2. Added support for consistent device naming for on-board devices.
3. Updated OOB module to R.1.0.1.3
4. Hid the item "Always Turbo Mode" after setting the "Turbo Mode" to disabled in Advanced/CPU Configuration page.
5. Added OEM strings to 50 bytes in type 11.
6. Added "Driver Health setup" item.
7. Added driver health warning message.
8. Renamed "AC Loss Policy Depend on" to "Restore on AC Power Loss".
9. Enhanced the solution for the error/warning message from dmidecode after AMIDE modification.
10. Enhanced Error logging for SD5.
11. Updated Coffee Lake-S R-0 stepping CPU microcode M22906ED_000000B4.
12. Updated SPS 5.1.03.62 for INTEL-SA-00213 Security Advisory to address CVE-2019-0089, CVE-2019-0090, CVE-2019-0086, CVE-2019-0091, CVE-2019-0092, CVE-2019-0093, CVE-2019-0094, CVE-2019-0096, CVE-2019-0097, CVE-2019-0098, and CVE-2019-0099.
13. Exposed the CPU's PL1 and PL2 items of Advanced -> CPU Configuration page in the BIOS setup menu.
14. Updated Intel RSTe RAID Option ROM/UEFI Driver to 6.1.0.1017.
15. Updated MCU 906EA-U0 + 906EB-B0 + 906EC-P0) for INTEL-SA-00233 Security Advisory to address CVE-2018-12126, CVE-2018-12127, and CVE-2018-12130.

16. Updated RC to version 7.0.58.41 to support 32GB of memory.
17. Updated USB and Fastboot module.
18. Set default setting Power Limit 2 to 150W when 8 Core CPU is used in the system.
19. Set OptionRom and boot mode select to EFI while CSM is disabled.
20. Changed UEFI LAN Boot option name format for SUM requirement.
21. Added RFC3021 solution for the network stack (/32 subnet mask support).
22. Fixed malfunction of SR-IOV feature.
23. Updated "Restore Optimized Defaults" string for Mehlow Server template.
24. Modified UEFI network description to IPv4/IPv6 to follow Industry Standard.
25. Removed processor version "Type" string for Mehlow Server template.
26. Added a Disabled option for "Onboard Video Option ROM" setup item.
27. Updated "Redirection After BIOS POST" string for Mehlow Server template.
28. Fixed problem of BMC VGA status being enabled in SMBIOS Type 41 when JPG1 is disabled (In 2-3).
29. Fixed lack of onboard VGA information in Type 40.
30. Fixed problem of DIMM location showing "NO DIMM INFO" in Event log when ECC error occurs.
31. Fixed problem of DIMM location always showing "DIMMA1" in BIOS Event log when ECC error occurs.
32. Fixed problem of the POST screen showing "?[1;31;40m" when EFI driver is "Unhealthy".
33. Fixed issue of system may or may not hanging up when LAN1 is disabled.

1.0a (12/24/2018)

1. Updated BIOS revision to 1.0a.
2. Updated Intel Reference Code to version 7.0.48.21.
3. Updated CPU MCUs (906EA, U0 + 906EB, B0 + 906EC, and P0).
4. Hid LAN OPROM Control items besides LAN#1 when LAN#1 OPROM is set to iSCSI.
5. Added Early Video messages when BIOS is in recovery mode.
6. Added "ACPI T-States" setup item.
7. Displayed "AERON" and "MCEON" strings during POST when "PCI AER Support" or "Memory Corrected Error" is enabled.
8. Hid "ECC Support" item.
9. Set the default of "Memory Corrected Error Enabling" to disabled.
10. Updated the Intel BIOS ACM version to 1.5.0 and SINIT ACM to 1.6.0.
11. Added "SMC SMBIOS Measurement" feature for PCR#1 measurement and enabled "Measure_Smbios_Tables".
12. Updated RAID option ROM and UEFI driver to 5.5.1028.
13. Added "MCEON" and "AERON" POST strings for SOL console when items are enabled.
14. Enhanced JPG1 function for running SUM with JPG1 2-3.
15. Added support for RFC4122 UUID format feature so that RFC4122 encoding from build time is produced by IPMICFG 1.29 tool or newer version.
16. Added SATA Frozen function.
17. Updated SPS firmware to SPS_E3_05.00.03.114.
18. Added support for Linux built-in utility efibootmgr.
19. Fixed inability of Boot Option of UEFI Application Boot Priorities to load default via Afu tool with command "/N".
20. Changed "Sata Interrupt Selection" default value to MSI.
21. Fixed problem of the status of Chassis Intru clearing in every single boot.
22. Fixed problem of serial port UID order not following COM port order after BIOS update.

23. Fixed problem of PCR#1 value changing during Legacy boot with TPM 2.0 when Measure_Smbios_Tables is disabled.
*24. Fixed problem of the system having an exception while entering BIOS Setup with NVMe M2*1 + SATA M2*1.*
25. Fixed problem of InBand receiving incorrect OEM FID size.
26. Fixed inability to show RSC-W-68 information when only RSC-W-68 is plugged in the SMBIOS.