# BIOS Release Notes Form



| | |
|---|---|
| **Product Name** | **X11SCH-(LN4)F** |
| **Release Version** | **2.2** |
| **Release Date** | **10/27/2023** |
| **Build Date** | **10/27/2023** |
| **Previous Version** | **2.1** |
| **Update Category** | **Recommended** |
| **Dependencies** | **None** |
| **Important Notes** | **None** |
| **Enhancements** | **1. Changed BIOS version to 2.2.**<br>**2. Updated for SA50199 changes to address CWE-20 (7.5 High).**<br>**3. Updated the UEFI VROC Driver to 8.0.0.4006.**<br>**4. Updated Microcode 906EA to 0xf6 and 906ED to 0xfc per IPU 2024.1.** |
| **New features** | **N/A** |
| **Fixes** | **1. Fixed NVMe devices not found when using legacy boot.**<br>**2. Rolled back SecureFlash and Smbios changes of SVN#1994.** |

***Release Notes from Previous Release(s)***

***2.1 (7/5/2023)***

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.*
4. *Ported code for supporting ofid check.*
5. *Corrected SUM_BIOS_OEM_FID_SUPPORT configure to SMC_OEMFID_SUPPORT.*

***2.0 (2/8/2023)***

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. *Updated 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 UefiNetworkStack to label 28 and add patch for AMI SA-50110 security issue.*
2. *Changed the setup string "SMCI" to "Supermicro", according to the new rule.*
3. *Updated DBX revocation packages released on UEFI.org on 08/15/2022 to fix Secure Boot Bypass issue.*
4. *Integrated 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 the failed automation test case "Check Https Boot".*
9. *Fixed resign fail during signing request.*

***1.8 (4/27/2022)***

1. *Changed BIOS version to 1.8.*
2. *Synched 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-TA-00615 to address CVE-2022-21166(5.5 High), CVE-2022-21123(6.1 High), CVE-2022-21127(5.6 High), for INTEL-TA-00617 to address CVE-2022-21151(5.3 High), for INTEL-TA-00614 to address CVE-2022-0005(4.9 High).*
4. *Updated Intel SINIT ACM to 1.10.1. For INTEL-TA-00601 to address CVE-2021-33123 (8.2 High), CVE-2021-33124 (7.5 High) security issues.*
5. *Updated SPS FW to SPS_E3_05.01.04.500 for IPU 2022.1.*

6. *Added support for IPMI UEFI PXE boot to all LAN ports.*
7. *Fixed the failure of the "FWTS-Live Test."*
8. *Fixed inability of SUM to get the BIOS setting "Software Guard Extensions (SGX)" via sum -c getcurrentbioscfg command.*

***1.6 (5/25/2021)***

1. *Changed the BIOS version to 1.6.*
2. *Updated SPS firmware to SPS_E3_05.01.04.303 for INTEL-TA-00459 Security Advisory to address CVE-2020-24509 (6.7, Medium) IPU 2021.1.*
3. *Copied the BIOS binary and renamed to adhere to 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-SA-00464 Security Advisory to address CVE-2020-24511 (5.6, Medium) and CVE-2020-24512 (2.8, Low) security issues.*
5. *Updated Intel BIOS ACM & SINIT ACM to 1.8.0 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.*
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 (11/17/2020)***

1. *Changed the BIOS version to 1.5.*
2. *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.*
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 Intel IPU 2020.2 RC 7.0.58.47 for Mehlow Refresh Server Platform Service Version.*
5. *Removed the FWSTS SMBIOS table.*
6. *Reduced Rowhammer susceptibility for AMI-SA50084 DDR4 Rowhammer vulnerability to address CVE-2020-10255 (9.0, high) security issue.*
7. *Patched inability of system to boot via onboard LAN2 after IPMI forces PXE boot when there is an OS behind LSI-3108 RAID card.*
8. *Added inband flash status event log to IPMI MEL.*
9. *Added Hotkey Message Enable/Disable function.*
10. *Enhanced SMCI HDD Security feature.*
11. *Updated SMBUS MUX setting.*
12. *Fixed problem of BIOS setup menu showing "Unknown" when plugging in the InnoDisk memory and boot up into BIOS setup menu.*
13. *Modified Intel Speed Shift Technology default to Disabled.*

***1.4 (5/26/2020)***

1. *Changed the BIOS version to 1.4.*
2. *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.*

3. *Updated Intel RSTe RAID Option ROM/UEFI Driver to 6.3.0.1005.*
4. *Implemented IPU 2020.1 update to SPS firmware to SPS_E3_05.01.04.113.0.*
5. *Enhanced the OEM FID feature to support UUID.*
6. *Disabled OPROM of internal graphics.*
7. *Added SMCI HDD Security feature.*
8. *Set the OverclockingLock flag to enabled by default for SGX test.*
9. *Added support for InnoDisk memory.*
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 RC to Mehlow Refresh PV version 7.0.58.44.*
3. *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.*
4. *Updated BiosAcm to 1.7.1 (20191213) and SinitAcm to 1.7.8 (20191220).*
5. *Added solution for problem of systems with LPDDR3 2133 MT/s DRAMs failing during boot.*
6. *Corrected the "DeepSx Power Policies" item string.*
7. *Displayed the "SGX Launch Control Policy" items in the BIOS setup menu.*
8. *Added SMC HDD Security feature.*
9. *Updated flag for skipping password prompt window.*
10. *Fixed inability of ME to enter recovery mode.*
11. *Fixed inability of BIOS to load default when plugging in M.2.*
12. *Added support for erasing NVMe Opal device (like Samsung 970 EVO model MZ-V7E250) without setting admin password.*

***1.2 (11/22/2019)***

1. *Changed BIOS version to 1.2.*
2. *Disabled the MCTP for buggy BMC workaround.*
3. *Updated Microcode M22906EA_000000CA (U-0 Stepping), M02906EB_000000CA (B-0 Stepping), and M22906EC_000000CA (P-0 Stepping) for INTEL-SA-00219 Security Advisory to address CVE-2019-0117 (6.0, Medium) security issue and for INTEL-SA-00220 Security Advisory to address CVE-2019-0123 (8.2, High) security issue.*
4. *Updated Microcode M22906ED_000000CA (R-0 Stepping) for INTEL-SA-00219 Security Advisory to address CVE-2019-0117 (6.0, Medium) security issue, Microcode M22906ED_000000CA (R-0 Stepping) for INTEL-SA-00220 Security Advisory to address CVE-2019-0123 (8.2, High) security issue, and Microcode M22906ED_000000CA (R-0 Stepping) for INTEL-SA-00270 Security Advisory to address CVE-2019-11135 (6.5, Medium) security issue.*
5. *Updated SPS firmware to SPS_E3_05.01.03.094.0.*

6. *Updated the Intel PMC firmware to 300.2.11.1022.*
7. *Updated the AMI TSE to 2.20.1276.*
8. *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.*
9. *Updated SINIT ACM to 1.7.4 for INTEL-SA-00240 to address CVE-2019-0151 (7.5 High) and CVE-2019-0152 (8.2 High), 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).*
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.*
11. *Removed "Hard Drive Security Frozen" setup item from SATA and RSTe Configuration page.*
12. *Added support for BMC AUX revision displaying.*
13. *Fixed problem of CECC being recorded in event log when METW is "60".*
14. *Fixed when use JPEG1 to disabled onboard VGA, and then boot into the operating system the onboard VGA device still exists.*
15. *Fixed inability to identify duplicate boot options with more than one of the same M.2 AHCI interface devices.*

***1.1 (8/20/2019)***

1. *Updated BIOS revision to 1.1.*
2. *Updated RC to Mehlow Refresh PV version 7.0.58.42.*
3. *Updated Coffee Lake-S R-0 stepping CPU microcode M22906ED_000000BE and Coffee Lake-S P-0 stepping CPU microcode M22906EC_000000BE.*
4. *Updated SPS firmware to SPS_E3_05.01.03.078.0.*
5. *Set memory uncorrectable error to always be recorded, regardless of METW and MECI.*
6. *Updated "Http Boot One Time" to "HTTP Boot One Time".*
7. *Added “SATA Frozen” function.*
8. *Updated SMC OOB module to 1.01.07, added Redfish/SUM Secure Boot feature, and updated OOB for secure boot and reserve Key.*
9. *Implemented dynamic change for Secure Boot Mode default value.*
10. *Fixed inability of BIOS to get SMBIOS type 39 power supply FRU data.*
11. *Fixed problem of key details showing "Security Violation" after loading Factory secure boot keys.*
12. *Fixed problem of two boot devices occurring in the boot order when installing UEFI CentOS.*
13. *Fixed failure of OPROM control item if CSM is disabled.*
14. *Fixed inability of system to find any network adapters and problem of the installation with vSphere aborting.*
15. *Fixed inability to enable TPM in the BIOS setup menu when plugging in TPM device and then disabling it.*
16. *Fixed problem of some items being adjusted when user adjusts dual boot order in BIOS setup.*
17. *Fixed inability to identify duplicated NVMe boot option with more than one of the same NVMe drives on an add-on card.*

***1.0b (5/24/2019)***

1. *Updated BIOS version to 1.0b.*
2. *Updated RC to version 7.0.58.41.*
3. *Updated Coffee Lake-S R-0 stepping CPU microcode M22906ED_000000B4.*

4. *Updated MCU (906EA-U0 + 906EB-B0 + 906EC-P0) for INTEL-SA-00233 Security Advisory to address CVE-2018-12126, CVE-2018-12127, CVE-2018-12130 and CVE-2019-11091 security issue.*
5. *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 security issue.*
6. *Updated Intel RSTe RAID Option ROM/UEFI Driver to 6.1.0.1017.*
7. *Updated SMC OOB module to support SMC LSI OOB Module.*
8. *Added Early Video messages when BIOS is in recovery mode.*
9. *Added "ACPI T-States" setup item.*
10. *Enhanced JPG1 function for running SUM with JPG1 2-3.*
11. *Enhanced "NVMe FW Source" function.*
12. *Added "Sata Frozen" function.*
13. *Added support for RFC4122 UUID format feature so that RFC4122 encoding from build time is produced by IPMICFG 1.29 tool or newer version.*
14. *Displayed "AERON" and "MCEON" string during POST when "PCI AER Support" or "Memory Corrected Error" is enabled.*
15. *Hid "ECC Support" item.*
16. *Set the default of "Memory Corrected Error Enabling" to Disabled.*
17. *Updated the Intel BIOS ACM version to 1.5.0 and SINIT ACM to 1.6.0.*
18. *Displayed Intel Graphics item and set the default value to Disabled.*
19. *Changed Package C State Limit default value to Auto and removed the C10 option.*
20. *Added "MCEON" and "AERON" POST string for SOL console when items are enabled.*
21. *Added support for Linux built-in utility efibootmgr.*
22. *Fixed problem of the system hanging in CP: 0xF4 when the system recovery occurs in BIOS with TPM module.*
23. *Updated BIOS Setup Menu for the item "Always Turbo Mode" in Advanced/CPU Configuration page.*
24. *Updated IPv4 and IPv6 setup items string.*
25. *Hid Serial Port 2 Attribute item if there is no real BMC COM.*
26. *Updated "Restore Optimized Defaults" string for Mehlow Server template.*
27. *Added "Driver Health" setup item.*
28. *Added Driver Health Warning message.*
29. *Updated to avoid inability to flash OA License Key randomly.*
30. *Renamed "AC Loss Policy Depend on" back to "Restore on AC Power Loss".*
31. *Enhanced the solution for the error/warning message from dmidecode after a modification by AMIDE.*
32. *Displayed the CPU's PL1 and PL2 items of Advanced -> CPU Configuration page in the BIOS setup menu.*
33. *Updated USB and Fastboot module.*
34. *Set default setting Power Limit 2 to 150W when 8 Core CPU is used in the system.*
35. *Set OptionRom and boot mode select to EFI while CSM is disabled.*
36. *Changed UEFI LAN Boot option name format for SUM requirement.*
37. *Added RFC3021 solution for the network stack (/32 subnet mask support).*
38. *Displayed the setup item "BME DMA Mitigation" in the Advanced -> PCIe/PCI/PnP Configuration page.*
39. *Fixed issue of serial port UID not following COM port order after BIOS update.*
40. *Fixed problem of InBand receiving incorrect OEM FID size.*
41. *Modified UEFI network description to IPv4/IPv6 to follow Industry Standard.*
42. *Removed processor version "Type" string for Mehlow Server template.*
43. *Added Disabled option for "Onboard Video Option ROM" setup item.*

44. *Fixed issue of onboard video having an output when JPG1 is disabled.*
45. *Updated "Redirection After BIOS POST" string for Mehlow Server template.*
46. *Fixed problem of BMC VGA status being enabled in SMBIOS Type 41 when JPG1 is disabled (In 2-3).*
47. *Fixed lack of onboard VGA information in Type 40.*
48. *Fixed issue of system using a constant 7-8% of the CPU when an interruption occurs.*
49. *Fixed issue of DIMM location showing "¡§No DIMM info¡" in Event Logs when ECC error occurs.*
50. *Fixed issue of ""?[1;31;40m" being shown on ] POST screen when EFI driver is "unhealthy".*
51. *Fixed problem of the value of Power Limit 2 displaying as 0 in setup menu when setup menu is set to 0 (AUTO).*
52. *Fixed inability of Intel Optane Memory M.2 to be detected.*
53. *Fixed issue of system may or may not hanging up when LAN1 is disabled.*
54. *Fixed issue of system recovery hanging up when TPM is installed.*
55. *Fixed issue of 4KN HDDs reporting 1TB when it should be 8TB.*