# BIOS Release Notes Form



| | |
|---|---|
| **Product Name** | **X11SCL-LN4F** |
| **Release Version** | **2.0** |
| **Release Date** | **2/17/2023** |
| **Build Date** | **2/17/2023** |
| **Previous Version** | **1.9** |
| **Update Category** | **Recommended** |
| **Dependencies** | **None** |
| **Important Notes** | **None** |
| **Enhancements** | **1. Modified Smbios eModule for Security update.**<br>**2. Modified CmosManager, ACHI, FlashSmi, HddSecurity, NVME, NVRAM, LegacySerialRedirection, OemActivation, Recovery, SecureFlash, TcgStorageSecurity, Smbios for Security update.**<br>**3. Modified SmmSmbiosElogInitFuncs.c for security update.**<br>**4. Updated Reference Code for Intel 2023.1 IPU.**<br>**5. Updated SPS FW to SPS_E3_05.01.04.804 for IPU 2023.1.**<br>**6. Changed BIOS version to 2.0.**<br>**7. Enabled Flash SMI support for the project.** |
| **New features** | **N/A** |

| | |
|---|---|
| **Fixes** | **N/A** |

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

***1.9 (9/12/2022)***

1. *Changed the setup string "SMCI" to "Supermicro", according to the new rule.*
2. *Updated DBX revocation packages released on UEFI.org on 08/15/2022 to fix Secure Boot Bypass issue.*
3. *Integrated IPU 2022.3 Reference Code IPU PV.*
4. *Updated SPS FW to SPS_E3_05.01.04.700.0 for IPU 2022.3.*
5. *Changed BIOS version to 1.9.*
6. *Updated 906ED Microcode to 0xF4 for IPU 2022.3.*
7. *Fixed resign fail during signing request.*

***1.8 (08/01/2022)***

1. *Enabled token "IPMI_FORCE_BOOT_UEFI_SHELL" to support shell by IPMI, changed boot order command.*
2. *Supports IPMI UEFI PXE boot to all LAN port feature.*
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_05.01.04.600.0 for IPU 2022.2.*
6. *Changed BIOS version to 1.8.*
7. *Updated UEFINetworkStack to label 28 and added patch for AMI SA-50110 security issue.*
8. *SUM cannot get the item "Software Guard Extensions (SGX)" from the BIOS configuration via sum -c getcurrentbioscfg command.*
9. *Fixed automation test case "Check Https Boot" fail.*

***1.6 (8/6/2021)***

1. *Changed the BIOS version to 1.6.*
2. *Updated Microcode M22906EA_000000EA (U-0 Stepping) for INTEL-SA-00464 Security Advisory to address CVE-2020-24512 (2.8, Low) security issue.*
3. *Updated SPS FW to SPS_E3_05.01.04.303 for INTEL-TA-00459 Security Advisory to address CVE-2020-24509 (6.7, Medium) IPU 2021.1.*
4. *Updated Intel BIOS ACM and 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.*
5. *Copied the BIOS binary and renamed it to meet the unique name format.*
6. *Fixed SUM test 220 fail due to "PCI AER Support" and "Memory Corrected Error Enabling" setting not preserved after flashing BIOS.*

***1.5 (10/05/2020)***

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. *Changed SPI TPM Clock Frequency to 17MHz for TPM detection.*
12. *Fixed problem of BIOS setup menu showing "Unknown" when plugging in the InnoDisk memory and boot up into BIOS setup menu.*

***1.4 (5/28/2020)***

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. *Fixed inability to change the serial port IO resource.*
10. *Fixed failure of Secure Erase password and problem of BIOS returning "EFI_Device_Error" with SED: Seagate ST1000NX0353.*

***1.3 (2/21/2020)***

1. *Added solution for problem of systems with LPDDR3 2133 MT/s DRAMs failing during boot.*
2. *Corrected the "DeepSx Power Policies" item string.*
3. *Updated RC to Mehlow Refresh PV version 7.0.58.44.*
4. *Displayed the "SGX Launch Control Policy" items in the BIOS setup menu.*
5. *Added SMC HDD Security feature.*
6. *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.*

7. *Updated flag for skipping password prompt window.*
8. *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).*
9. *Fixed inability of ME to enter recovery mode.*
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 (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. *Fixed problem of CECC being recorded in event log when METW is "60".*

***1.1 (8/28/2019)***

1. *Changed the BIOS version to 1.1.*
2. *Set memory uncorrectable error to always be recorded, regardless of METW and MECI.*
3. *Updated SPS firmware to SPS_E3_05.01.03.078.0.*
4. *Added "SATA Frozen" function.*
5. *Updated SMC OOB module to 1.01.08, added Redfish/SUM Secure Boot feature, and updated OOB for secure boot and reserve Key.*
6. *Updated RC to Mehlow Refresh PV version 7.0.58.42.*
7. *Implemented dynamic change for Secure Boot Mode default value.*

8. *Fixed inability of BIOS to get SMBIOS type 39 power supply FRU data.*
9. *Updated Coffee Lake-S R-0 stepping CPU microcode M22906ED_000000BE and Coffee Lake-S P-0 stepping CPU microcode M22906EC_000000BE.*
10. *Displayed setup item "BME DMA Mitigation" on the Advanced -> PCIe/PCI/PnP Configuration page.*
11. *Fixed problem of SATA Configuration page showing 1TB for 8TB 4KN HDDs.*
12. *Fixed problem of key details showing "Security Violation" after loading Factory secure boot keys.*
13. *Fixed problem of two boot devices occurring in the boot order when installing UEFI CentOS.*
14. *Fixed failure of OPROM control item if CSM is disabled.*
15. *Fixed inability of system to find any network adapters and problem of the installation with vSphere aborting.*
16. *Fixed inability to enable TPM in the BIOS setup menu when plugging in TPM device and then disabling it.*
17. *Fixed problem of some items being adjusted when user adjusts dual boot order in BIOS setup.*
18. *Fixed inability to identify duplicated NVMe boot option with more than one of the same NVMe drives on an add-on card.*

***1.0b (5/17/2019)***

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_000000B0.*
4. *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.*
5. *Update 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.*
6. *Update 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.*
7. *Updated Intel RSTe RAID Option ROM/UEFI Driver to 6.1.0.1017.*
8. *Updated USB and Fastboot module.*
9. *Enhanced the solution for the error/warning message from dmidecode after a modification by AMIDE.*
10. *Exposed the CPU's PL1 and PL2 items of Advanced -> CPU Configuration page in the BIOS setup menu.*
11. *Renamed "AC Loss Policy Depend on" back to "Restore on AC Power Loss".*
12. *Updated to avoid inability to flash OA License Key randomly.*
13. *Added Driver Health setup item.*
14. *Added driver health warning message.*
15. *Added OEM strings to 50 bytes in Type 11.*
16. *Updated IPv4 and IPv6 setup items string.*
17. *Updated BIOS Setup Menu for the item "Always Turbo Mode" in Advanced/CPU Configuration page.*
18. *Added code for Consistent Device Name support.*
19. *Added support for Linux built-in utility efibootmgr.*
20. *Set default setting Power Limit 2 to 150W when 8 Core CPU is used in the system.*
21. *Set OptionRom and boot mode select to EFI while CSM is disabled.*
22. *Changed UEFI Lan Boot option name format for SUM requirement.*

23. *Added RFC3021 solution for the network stack (/32 subnet mask support).*
24. *Exposed the setup item "BME DMA Mitigation" in the Advanced -> PCIe/PCI/PnP Configuration page.*
25. *Fixed issue of DIMM location to show "¡§No DIMM infoj" in Event Logs when ECC error occurs.*
26. *Fixed issue of DIMM location to always show "DIMMA1" in BIOS Event log when ECC error occurs.*
27. *Fixed issue of ""?[1;31;40m" being shown on POST screen when EFI driver is "unhealthy".*
28. *Fixed issue of BMC VGA status showing Enabled in SMBIOS Type 41 when JPG1 is disabled (In 2-3).*
29. *Fixed issue of onboard video having an output when JPG1 is disabled.*
30. *Fixed problem of hot-plug being registered when the PCH root port bridge is without a PCI-E device.*
31. *Updated "Restore Optimized Defaults" string for Mehlow Server template.*
32. *Modified UEFI network description as IPv4/IPv6 to follow Industry Standard.*
33. *Added workaround for BIOS flash failure with 156 bytes PubKey (Error: "Secure Flash Rom Verify Fail").*
34. *Fixed problem of the system hanging in CP: 0xF4 when the system recovery occurs in BIOS with TPM module.*
35. *Fixed problem of the value of Power Limit 2 displaying as 0 in setup menu when setup menu is set to 0 (AUTO).*
36. *Fixed issue of system may or may not hanging up when LAN1 is disabled.*
37. *Fixed DIMM location of ECC error to show "NO DIMM INFO" in Event log when Multi-Bit ECC error occurs.*

***1.0a (2/26/2019)***

1. *Updated BIOS revision to 1.0a.*
2. *Updated Intel Reference Code to version 7.0.51.40.*
3. *Updated CPU MCU (906EA, U0 + 906EB, B0 + 906EC, P0).*
4. *Hid LAN OPROM Control items 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. *Hide "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. *Added support for Linux built-in utility efibootmgr.*
18. *Hid "Always Turbo Mode" when "Turbo Mode" setting is set to Disable in Advanced/CPU Configuration page.*
19. *Updated IPv4 and IPv5 setup item strings.*
20. *Added OEM strings to 50 bytes in Type 11.*
21. *Added Disabled option for "Onboard Video Option ROM" setup item.*

22. *Added "Driver Health" setup item.*
23. *Added Driver Health warning message.*
24. *Renamed "AC Loss Policy Depend on" to "Restore on AC Power Loss".*
25. *Enhanced the solution for the error/warning message from dmidecode after AMIDE modification.*
26. *Updated SMBIOS Type 9 for AOC Sensor Reading.*
27. *Fixed inability to Boot Option of UEFI Application Boot Priorities to load default via Afu tool with command "/N".*
28. *Changed the "SATA Interrupt Selection" default value to MSI.*
29. *Fixed problem of Chassis Intrusion status in BMC clearing every time system boots.*
30. *Fixed issue of serial port UID order to follow COM port order after BIOS update.*
31. *Fixed issue of PCR#1 value to be changed during Legacy boot with TPM 2.0 when Measure_Smbios_tables is disabled.*
32. *Fixed problem of the system having an exception while entering BIOS Setup with NVMe M2*1 + SATA M2*1.*
33. *Fixed problem of InBand receiving incorrect OEM FID size.*
34. *Fixed problem of system hanging in CP during system recovery BIOS with TPM module.*
35. *Updated "Restore Optimized Defaults" string for Mehlow Server template.*
36. *Modified UEFI network description to IPv4/IPv6 to follow Industry Standard.*
37. *Removed processor version "Type" string for Mehlow Server template.*
38. *Fixed issue of onboard video output displaying screen on DXE stage when JPG1 is disabled.*
39. *Updated "Redirection After BIOS POST" string for Mehlow Server template.*
40. *Fixed problem of BMC VGA status being enabled in SMBIOS Type 41 when JPG1 is disabled (In 2-3).*
41. *Fixed lack of onboard VGA information in Type 40.*