BIOS Release Notes Form

Product Name	**X11SCL-IF**
Release Version	**2.0**
Release Date	**2/23/2023**
Build Date	**2/23/2023**
Previous Version	**1.9**
Update Category	**Recommended**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. 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.
New features	**N/A**
Fixes	**N/A**

Release Notes from Previous Release(s)

1.9 (9/22/2022)

1. "SMCI" strings are now "Supermicro"
2. Updated DBX revocation packages released on UEFI.org on 8/15/2022 to fixed Secure Boot Bypass issue.
3. Integration for IPU 2022.3 Rference 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 the resign function after a sign request.

1.8 (6/24/2022)

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-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. Supported IPMI UEFI PXE boot to all LAN port feature.
7. Updated UefiNetworkStack to label 28 and add patch for AMI SA-50110 security issue.
8. Added SmcNetworkOpRomFlag for projects which don't contain onboard LAN to dynamically enable Uefi of slot which connects to the NIC when HttpBoot is set through SUM.
9. Fixed automation test case "Check Https Boot."
10. Checked SMBIOS log information, it displayed "DIMMB1".

1.6 (5/31/2021)

1. Change BIOS version to 1.6.
2. Update Microcode M22906EA_000000EA (U-0 Stepping) for INTEL-SA-00464 Security Advisory to address CVE-2020-24512(2.8, Low) security issue.
3. Update 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. Update 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.
5. Copy the BIOS binary and rename to meet the unique name format.
6. Added x-ami for "PCI AER Support" and "Memory Corrected Error Enabling" setup items.

1.5 (10/5/2020)

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. Reduced Rowhammer susceptibility for AMI-SA50084 DDR4 Rowhammer vulnerability to address CVE-2020-10255 (9.0, high) security issue.
9. Fixed problem of BIOS setup menu showing "Unknown" when plugging in the InnoDisk memory and boot up into BIOS setup menu.

1.4 (5/27/2020)

1. Changed the BIOS version to 1.4.
2. Enhanced the OEM FID feature to support UUID.
3. Implemented IPU 2020.1 update to SPS firmware to SPS_E3_05.01.04.113.0.
4. Added SMCI HDD Security feature.
5. 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.
6. Set the OverclockingLock flag to enabled by default for SGX test.
7. Added support for InnoDisk memory.
8. Updated Intel RSTe RAID Option ROM/UEFI Driver to 6.3.0.1005.
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 (10/24/2019)

1. Changed BIOS version to 1.2.
2. Added support for BMC AUX revision displaying.
3. 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.
4. 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.
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 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, Midium) security issue.

1.0b (5/24/2019)

1. Changed BIOS version to 1.0b.
2. Updated Coffee Lake-S R-0 stepping CPU microcode M22906ED_000000B4.
3. 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.
4. Displayed the CPU's PL1 and PL2 items of Advanced -> CPU Configuration page in the BIOS setup menu.
5. Updated Intel RSTe RAID Option ROM/UEFI driver to 6.1.0.1017.
6. 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.
7. Updated RC to version 7.0.58.41.
8. Updated USB and Fastboot module.
9. Enhanced the solution for the error/warning message from dmidecode after a modification by AMIDE.
10. Renamed "AC Loss Policy Depend on" back to "Restore on AC Power Loss".
11. Updated to avoid inability to flash OA License Key randomly.
12. Added Driver Health setup item.
13. Added Driver Health warning message.
14. Added OEM strings to 50 bytes in Type 11.
15. Updated IPv4 and IPv6 setup items string.
16. Updated BIOS Setup Menu for the item "Always Turbo Mode" in Advanced/CPU Configuration page.
17. Added code for Consistent Device Name support.
18. Added support for Linux built-in utility efibootmgr.

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 issue of DIMM location showing "¡§No DIMM info¡" in Event Logs when ECC error occurs.
23. Fixed issue of DIMM location to always show "DIMMA1" in BIOS Event log when ECC error occurs.
24. Fixed issue of ""?[1;31;40m" being shown on POST screen when EFI driver is "unhealthy".
25. Fixed problem of BMC VGA status being enabled in SMBIOS Type 41 when JPG1 is disabled (In 2-3).
26. Fixed issue of onboard video having an output when JPG1 is disabled.
27. Fixed problem of hot-plug being registered when the PCH root port bridge is without a plug in add-on card.
28. Updated "Restore Optimized Defaults" string for Mehlow Server template.
29. Modified UEFI network description to IPv4/IPv6 to follow Industry Standard.
30. Added workaround for BIOS flash failure with 156 bytes PubKey (Error: "Secure Flash Rom Verify Fail").
31. Fixed problem of the system hanging in CP: 0xF4 when the system recovery occurs in BIOS with TPM module.
32. Fixed problem of the value of Power Limit 2 displaying as 0 in setup menu when setup menu is set to 0 (AUTO).
33. Fixed issue of system may or may not hanging up when LAN1 is disabled.
34. Fixed issue of system recovery hanging up when TPM is installed.
35. Fixed abnormal issue of DMI Type 17 data.

1.0a (12/19/2018)

1. Added a CallBack for enabling Secure Boot.
2. Added Early Video messages when BIOS is in recovery mode.
3. Added "ACPI T-States" setup item.
4. Enhanced JPG1 function for running SUM with JPG1 2-3.
5. Enhanced "NVMe FW Source" function.
6. Added support for RFC4122 UUID format feature so that RFC4122 encoding from build time is produced by IPMICFG 1.29 tool or newer version.
7. Added SATA Frozen function.
8. Displayed "AERON" and "MCEON" strings during POST when "PCI AER Support" or "Memory Corrected Error" is enabled.
9. Hid "ECC Support" item.
10. Set the default of "Memory Corrected Error Enabling" to disabled.
11. Updated the Intel BIOS ACM version to 1.5.0 and SINIT ACM to 1.6.0.
12. Added ability to use token to define the GPIO for PEG port reset.
13. Updated Intel Reference Code to version 7.0.48.21.
14. Added "SMC SMBIOS Measurement" feature for PCR#1 measurement and enabled "Measure_Smbios_Tables".
15. Added "MCEON" and "AERON" POST strings for SOL console when items are enabled.
16. Fixed abnormal function of LAN2 PXE.
17. Updated RAID option ROM and UEFI driver to 5.5.1028.
18. Fixed inability of Boot Option of UEFI Application Boot Priorities to load default via Afu tool with command "/N".
19. Changed "Sata Interrupt Selection" default value to MSI.

20. Fixed problem of serial port UID order not following COM port order after BIOS update.
21. Fixed problem of PCR#1 value changing during Legacy boot with TPM 2.0 when Measure_Smbios_Tables is disabled.
22. Revised SA/PCH Configuration Page Form Set GOTO setting.
23. Fixed problem of InBand receiving incorrect OEM FID size.