IPMI Firmware / BIOS Release Notes Form

Product Name	**X11SCM-(LN8)F**
Release Version	**1.3**
Release Date	**2/28/2020**
Build Date	**2/28/2020**
Previous Version	**1.2**
Update Category	**Critical**
Dependencies	**None**
Important Notes	**None**
Enhancements	**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. Corrected the "DeepSx Power Policies" item string.** **4. Updated RC to Mehlow Refresh PV version 7.0.58.44.** **5. Displayed the "SGX Launch Control Policy" items in the BIOS setup menu.** **6. Added SMC HDD Security feature.** **7. 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. **8. Updated flag for skipping password prompt window.** **9. Updated SPS firmware to SPS_E3_05.01.04.104.0.**
New features	**None**
Fixes	**1. Fixed inability of BIOS to load default when plugging in M.2.** **2. Added support for erasing NVMe Opal device (like Samsung 970 EVO model MZ-V7E250) without setting admin password.**

Release Notes from Previous Release(s)

1.2 (10/22/2019)

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, Midium) security issue.

1.0b (5/17/2019)

1. Updated BIOS revision 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, and CVE-2018-12130.
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.

6. Updated Intel RSTe RAID Option ROM/UEFI driver to 6.1.0.1017.
7. Updated USB and Fastboot module.
8. Enhanced the solution for the error/warning message from dmidecode after a modification by AMIDE.
9. Displayed the CPU's PL1 & PL2 items of Advanced -> CPU Configuration page on the BIOS setup menu.
10. Renamed "AC Loss Policy Depend on" to "Restore on AC Power Loss".
11. Prevented random inability to flash OA License Keys.
12. Added Driver Health setup item.
13. Added driver health warning message.
14. Updated SMBIOS type 11 OEM string size to 50 bytes.
15. Updated IPv4 and IPv6 setup item strings.
16. Hid the item "Always Turbo Mode" after setting the "Turbo Mode" to disabled in Advanced/CPU Configuration page.
17. Added code for consistent device name support.
18. Added support for Linux built-in utility efibootmgr.
19. Added setting of system default Power Limit 2 to 150W when using 8 Core CPU.
20. Set OptionRom and boot mode selection to EFI while CSM is disabled.
21. Changed UEFI LAN Boot option name format.
22. Displayed setup item "BME DMA Mitigation" on the Advanced -> PCIe/PCI/PnP Configuration page.
23. Fixed problem of DIMM location of ECC error showing "NO DIMM INFO" in Event log when Multi-Bit ECC error occurs.
24. Fixed problem of "?[1;31;40m" showing on POST screen when EFI driver is "Unhealthy".
25. Fixed problem of the status of BMC VGA showing as enabled in SMBIOS Type 41 when JPG1 is disabled (on 2-3).
26. Fixed problem of onboard video showing output when JPG1 disabled.
27. Updated “Restore Optimized Defaults” string for Mehlow Server template.
28. Modified UEFI network description to IPv4/IPv6 to follow Industry Standard.
29. Fixed failure of workaround for BIOS flash with 156 bytes PubKey (Error: “Secure Flash Rom Verify Fail”).
30. Fixed problem of the system hanging in CP: 0xF4 when the system recovery occurs in BIOS with TPM module.
31. Fixed problem of the value of Power Limit 2 displaying as 0 in setup menu when setup menu is set to 0 (AUTO).
32. Fixed problem of system hanging when disabling LAN1.

1.0a (12/18/2018)

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. Fixed inability of Boot Option of UEFI Application Boot Priorities to load default via Afu tool with command "/N".
18. Changed "Sata Interrupt Selection" default value to MSI.
19. Fixed problem of the status of Chassis Intru clearing in every single boot.
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. Fixed problem of the system hanging up at b2h when all add-on devices are needed to use IO resource.
*23. Fixed problem of the system having an exception while entering BIOS Setup with NVMe M2*1 + SATA M2*1.*
24. Fixed problem of InBand receiving incorrect OEM FID size.