BIOS Release Notes Form

Supermicro disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade. All products, computer systems, dates, and figures specified are preliminary based on current expectations, and are subject to change without notice. Supermicro and the Supermicro logo are trademarks of Super Micro Computer, Inc. in the U.S. and/or other countries. Copyright © 2018 Super Micro Computer, Inc. All rights reserved.

Product Name	**X11SCM-(LN8)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	**N/A**
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. *Updated 906ED Microcode to 0xF4 for IPU 2022.3.*
2. *Modified Smbios eModule for Security update.*
3. *Modified CmosManager, ACHI, FlashSmi, HddSecurity, NVME, NVRAM, LegacySerialRedirection, OemActivation, Recovery, SecureFlash, TcgStorageSecurity, Smbios for Security update.*
4. *Modified SmmSmbiosElogInitFuncs.c for security update.*
5. *Updated Reference Code for Intel 2023.1 IPU.*
6. *Updated SPS FW to SPS_E3_05.01.04.804 for IPU 2023.1.*
7. *Changed BIOS version to 2.0.*
8. *Enabled Flash SMI support for the project.*

1.9 (9/16/2022)

1. *According to new rule, changed setup string "SMCI" to "Supermicro."*
2. *Updated DBX revocation packages released on UEFI.org on 08/15/2022 to fix Secure Boot Bypass issue.*
3. *Integration for 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 when request sign.*

1.8 (5/23/2022)

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. *Supported IPMI UEFI PXE boot to all LAN port feature.*
6. *Updated SPS FW to SPS_E3_05.01.04.600.0 for IPU 2022.2.*
7. *Added SmcNetworkOpRomFlag for projects which don't contain onboard LAN to dynamically enable Uefi of slot which is connect to NIC when HttpBoot is set through SUM.*

1.6 (5/28/2021)

1. *Changed BIOS version to 1.6.*
2. *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.*
3. *Copied the BIOS binary and rename to meet the unique name format.*
4. *Updated Microcode M02906EB_000000EA (B-0 Stepping), M22906EC_000000EA (P-0 Stepping) and M22906ED_000000EA (R-0 Stepping) for Intel 20211IPU.*

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. *Added x-ami for "PCI AER Support" and "Memory Corrected Error Enabling" setup items.*

1.5 (10/5/2020)

1. *Changed the BIOS version to 1.5.*
2. *Added "SMC_PATCH_SECUREFLASH_UNMAPPED_REGION" patch to fix failure of BIOS flash with module SecureFlash_23.*
3. *Added inband flash status event log to IPMI MEL.*
4. *Added Hotkey Message Enable/Disable function.*
5. *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.*
6. *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.*
7. *Updated Intel IPU 2020.2 RC 7.0.58.47 for Mehlow Refresh Server Platform Service Version.*
8. *Removed the FWSTS SMBIOS table.*
9. *Enhanced SMCI HDD Security feature.*
10. *Reduced Rowhammer susceptibility for AMI-SA50084 DDR4 Rowhammer vulnerability to address CVE-2020-10255 (9.0, high) security issue.*
11. *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. *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 (1/28/2020)

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. *Updated SPS firmware to SPS_E3_05.01.04.104.0.*
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 (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.*