

## IPMI Firmware / 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.*

<b>Product Name</b>	<b>X11SCL-IF</b>
<b>Release Version</b>	<b>1.2</b>
<b>Release Date</b>	<b>10/24/2019</b>
<b>Build Date</b>	<b>10/24/2019</b>
<b>Previous Version</b>	<b>1.0b</b>
<b>Update Category</b>	<b>Critical</b>
<b>Dependencies</b>	<b>None</b>
<b>Important Notes</b>	<b>None</b>
<b>Enhancements</b>	<ol style="list-style-type: none"><li>1. Changed BIOS version to 1.2.</li><li>2. Added support for BMC AUX revision displaying.</li><li>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.</li><li>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.</li><li>5. Updated SPS firmware to SPS_E3_05.01.03.094.0.</li><li>6. Updated the Intel PMC firmware to 300.2.11.1022.</li><li>7. Updated the AMI TSE to 2.20.1276.</li></ol>

	<p><b>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.</b></p> <p><b>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.</b></p>
<b>New features</b>	N/A
<b>Fixes</b>	N/A

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

### **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 "i\$No DIMM infoj" 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.