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.

Product Name	**X11SSA-F/X11SSi-LN4F**
Release Version	**2.2a**
Release Date	**5/23/2019**
Previous Version	**2.2**
Update Category	**Critical**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Updated Intel CPU microcode from DT_P_183 for INTEL-SA00233 Security Advisory.** **2. Updated EIP419363 to ensure DCI Policy is "Disabled" for INTEL-SA-00127, EIP412144 for [SA50044] USRT Mantis vulnerabilities, EIP387724 for Ofbd Meud Security vulnerabilities, and EIP422042 for CPU microcode downgrade attack vulnerability.** **3. Updated Greenlow Refresh Initialization Code PV PLR5 Hotfix1 version 4.1.1.1 for INTEL-SA-00223 Security Advisory to address CVE-2019-0119, CVE-2019-0120, and CVE-2019-0126 security issues.** **4. Contained SPS 4.01.04.054 PLR version for security vulnerability INTEL-SA-00213.** **5. Updated Kaby Lake BIOS ACM 1.5.0 and SINIT ACM 1.6.0.** **6. Updated EIP393007 & EIP411789 for TPM vulnerability when resuming S3.**

	7. Updated SATA RAID OPROM/EFI driver to RSTe PreOS v4.7.0.1017. 8. Updated VBIOS and VGA EFI Driver to 1.09 to fix ASpeed CVE-2019-6260 security issue. 9. Updated valid range of IPMI setup item VLAN ID to 1-4094. 10. Added support for RFC4122 UUID format feature to set RFC4122 encoding from build time produced by IPMICFG 1.29 tool or newer.
New features	N/A
Fixes	1. Fixed problem of BIOS always retrying boot when Re-Try Boot is Disabled. 2. Fixed inability to disable SMBIOS preservation for recovery. 3. Fixed inability to log CECC events in IPMI event log when METW = 0.

Release Notes from Previous Release(s)

2.2 (5/23/2018)

1. Updated CPU microcode to address 'Spectre' derivatives (CVE-2018-3639 & CVE-2018-3640) security issue.
2. Updated Kaby Lake BIOS ACM 1.4.0 and SINIT ACM 1.3.0.
3. Enhanced ability to enter setup menu without password when system only has Administrator password.
4. Fixed problem of the system hanging when trying to create virtual driver on LSI3108 storage card under BIOS setup.
5. Implemented workaround for problem of IP displaying 0.0.0.0 information the first time AC powers on BMC.
6. Fixed problem of Afu /O command clearing SMC SMBIOS region ($SMC).
7. Fixed missing reminding string "iKVM doesn't support add-on VGA device..." when VGA is plugged in & "Primary Display"=="PEG".

2.1a (02/12/2018)

1. Updated DT_B_128 for Kaby Lake-S B0 stepping CPU microcode M2A906E9_00000084 to address 'Spectre' variant 2 (CVE 2017-5715) security issue.
2. Added support for UEFI mode PXE boot via F12 hot key Net boot.
3. Added support for SUM to display SGX-related items.
4. Added AOC-SLG3-2M2 1.01 into NVMe table for auto bifurcation.
5. Added Ramaxel JEDEC Manufacturer ID to support Ramaxel memory.
6. Fixed inability to load Broadcom SAS3008 configuration utility.
7. Fixed issue of all commands requesting to be persistent.
8. Fixed issue with IPMI force boot.

2.1 (12/10/2017)

1. Updated DT_P_140 for Kaby Lake-S B0 stepping MCU M2A906E9_0000007C and Skylake-S R0/S0 stepping MCU M36506E3_000000C2.
2. Updated SATA RAID OPROM/EFI driver to RSTe PreOS v4.7.0.1014 (RSTe SATA 4.7.0.1069 and NVMe 4.7.0.2063).
3. Fixed problem of ACPI Exception: AE_NOT_FOUND occurring.