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	**X11DSF-E**
Release Version	**3.1 SPS: 4.1.04.256**
Release Date	**05/02/2019**
Previous Version	**3.0a**
Update Category	**Recommended**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Updated Skylake-SP/Cascade Lake-SP CPU microcode.** **2. Updated Intel BKCWW16 2019 PV PLR1.** **3. Updated SPS_E5_04.01.04.296.0 from BKC WW16 2019.** **4. Displayed 3rd IPMI version in BIOS setup.** **5. Set SDDC Plus One or SDDC to disabled by default.** **6. Updated SATA/sSATA RAID OPROM/EFI driver to VROC PreOS v6.1.0.1017.** **7. Changed OPROM settings to EFI for OEM BIOS that only changes the boot mode to UEFI without other changes.** **8. Enhanced the solution for the error/warning message from dmidecode after a modification by AMIDE.** **9. Enhanced BIOS setup menu to auto-switch the Option ROM's value and hide the unexpected value when boot mode changes.** **10. Enhanced BIOS setup menu to switch the boot mode value and**

	Option ROM's values when CSM support is disabled and applied this to enabled secure boot mode case. 11. Set ADDDC to enabled by default.
New features	N/A
Fixes	1. Fixed problem of the system equipped with dTPM 2.0 hanging up at POST code 0x90 when disabling dTPM 2.0 by SUM TPM OOB command "--disable_dtpm". 2. Modified UEFI network description to IPv4/IPv6 to follow Industry Standard. 3. Fixed problems of system hanging up at POST code 0x92 and rebooting endlessly during POST and inability to get PPIN under OS (DOS/EFI shell/Windows/Linux). 4. Fixed failure to log memory UCE event due to incorrect flag. 5. Fixed inability of "Network Stack"-related items to get/change via SUM OOB method. 6. Fixed incorrect display of the TDP of Intel Speed Select table. 7. Temporarily fixed error for SKX (CLX) 4114 CPU memory training with Micron (18ASF2G72PDZ-2G6E1) RDIMM. 8. Fixed failure to boot into VMware OS when set to Maximum Performance even if Monitor/MWAIT is enabled.

Release Notes from Previous Release(s)

3.0a (2/16/2019)

1. Added support for Purley Refresh platform.
2. Updated AMI label 5.14_PurleyCrb_0ACLA038_BETA (BKC WW50).
3. Added support for Monitor Mwait feature.
4. Patched missing PSU information if backplane MCU reports wrong PSU information.
5. Disabled "tRWSR Relaxation" by default.
6. Set PCIe correctable and uncorrectable (non-fatal) error report to disabled by default.
7. Added support for RFC4122 UUID format feature to set RFC4122 encoding from build time produced by IPMICFG 1.29 tool or newer.
8. Disabled PCH "PCI-E Global ASPM Support".
9. Set NVDIMM ADR timeout to 600us according to Intel PDG.
10. Fixed malfunction of disabling Watch Dog while flashing BIOS under OS.
11. Fixed problem of BIOS always retrying boot when Re-Try Boot is Disabled.
12. Fixed malfunction of support for LEGACY to EFI.
13. Fixed failure of always turbo in new Linux kernel 7.2.
14. Added workaround for failure of BIOS flash with 156 bytes PubKey (Error: "Secure Flash Rom Verify Fail").
15. Fixed failure of CPU PBF (Prioritized Base Frequency).
16. Fixed issue with the backplane NF1 NVMe hot plug-in.

2.1 (8/24/2018)

1. Updated CPU microcode to address 'Spectre' derivatives (CVE-2018-3639 & CVE-2018-3640) security issue.
2. Enabled BIOS secure flash upgrade feature (firmware signature).
3. Corrected BIOS/ME downgrade check for SPS 4.0.4.340 and later.
4. Displayed Memory DIMM PPR setup item.
5. Checked PCH SKU for QAT enabled board.
6. Added message "Secure Flash Recovery Image Verification Failed." for prompting user if secure flash recovery image is invalid.
7. Updated SPS 4.0.4.381 for INTEL-SA-00131 Security Advisory to address CVE-2018-3643 and CVE-2018-3644 security issues.
8. Fixed failure of WDT function.
9. Fixed inability of system to clean event log via Afu command "/CLNEVNLOG".
10. Fixed issue with IPMI firmware to enable storage card to show temperature.