# 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** | **X11DPU-Z+** |
| **Release Version** | **3.2 SPS: 4.1.04.339** |
| **Release Date** | **10/22/2019** |
| **Build Date** | **10/22/2019** |
| **Previous Version** | **3.1** |
| **Update Category** | **Recommended** |
| **Dependencies** | **None** |
| **Important Notes** | **None** |
| **Enhancements** | **1. Updated AMI label 5.14_PurleyCrb_0ACLA049_BETA for BKC WW36 RC595.D04 for AMI security update SA50072, IPU 2019.2 INTEL-SA-00280 Security Advisory to address CVE-2019-11136 (7.5, High) and CVE-2019-11137 (7.5, High) security issues.**<br>**2. Updated SINIT ACM 1.7.3 PW from BKC WW36 IPU 2019.2 for INTEL-SA-00240 Security Advisory to address CVE-2019-0151 (7.5, High) and CVE-2019-0152 (8.2, High) security issues.**<br>**3. Updated SPS_E5_04.01.04.339.0 from BKC WW36 IPU 2019 for INTEL-SA-00241 Security Advisory to address CVE-2019-11090 (6.8, Medium), CVE-2019-11088 (7.5, High), CVE-2019-0165 (4.4, Medium), CVE-2019-0166 (5.9, Medium), CVE-2019-0168 (4.6, Medium), CVE-2019-0169 (9.6, Critical), CVE-2019-11086 (3.5, Low), CVE-2019-11087 (6.4, Medium), CVE-2019-11101 (4.4, Medium), CVE-2019-11100 (6.1, Medium), CVE-2019-11102 (4.1, Medium), CVE-2019-11103 (7.3, High), CVE-2019-11104 (7.3, High), CVE-2019-11105 (7.9, High), CVE-** |

| | |
|---|---|
| | **2019-11106 (4.4, Medium), CVE-2019-11107 (5.3, Medium), CVE-2019-11108 (2.3, Low), CVE-2019-11110 (4.1, Medium), CVE-2019-11097 (7.3, High), CVE-2019-0131 (7.1, High), CVE-2019-11109 (4.4, Medium), CVE-2019-11131 (7.5, High), CVE-2019-11132 (8.4, High), and CVE-2019-11147 (8.2, High) security issues.**<br>**4. Updated Skylake-SP/Cascade Lake-SP CPU microcode from Intel-Generic-Microcode-20191004_NDA for INTEL-SA-00271 Security Advisory to address CVE-2019-11139 (5.8, Medium) security issue.**<br>**5. Fixed ability to see memory correctable error event during MRC when use a single bit bad DIMM.**<br>**6. Changed "Secure Boot Mode" to ReadOnly attribute.**<br>**7. Displayed Setup item "ARI Support".**<br>**8. Prevented SDDC and ADDDC from graying out when Run Sure is enabled.**<br>**9. Added support for firmware version information.**<br>**10. Fixed mismatch of Secure Boot value.**<br>**11. Fixed problem of setup pages disappearing after ReadyToBoot.**<br>**12. Set software threshold for non-fatal MCE error with yellow status to enabled as default.**<br>**13. Enhanced support for Intel Speed Select.**<br>**14. Implemented dynamic change for Secure Boot Mode default value.**<br>**15. Added support for keeping Linux MOK keys database.**<br>**16. Added Redfish/SUM Secure Boot feature to update OOB for secure boot and reserve Key.**<br>**17. Updated VBIOS and VGA EFI Driver to 1.10.**<br>**18. Added recommended AEP DIMM firmware version.**<br>**19. Updated SATA/sSATA RAID OPROM/EFI driver to VROC PreOS v6.2.0.1034.**<br>**20. Disabled ADDDC/SDDC and set PPR as hPPR.**<br>**21. Updated RC595.D04 hot fix.** |

|  |  |
|---|---|
| New features | 1. Added Enhanced PPR function. |
| Fixes | 1. Removed PXE option for "OnBoard LanX Option ROM" when "Boot mode select" is UEFI.<br>2. Fixed inability of InBand Update BIOS in Linux OS to preserve Linux secureboot keys.<br>3. Corrected display of the IPMI AUX revision.<br>4. Fixed problem of boot time increasing by more than two minutes per boot after running stress over hundreds of cycles.<br>5. Fixed inability to identify duplicated NVMe boot option with more than one of the same NVMe drives on an add-on card.<br>6. Changed OOB download and Upload Bios Configuration sequence.<br>7. Fixed failure of the default boot order of UEFI groups to sync when "Boot mode" is under UEFI mode.<br>8. Fixed problem of key details showing "Security Violation" after loading Factory secure boot keys.<br>9. Masked AP Mwait instruction if needed.<br>10. Removed SNC override when set to extreme performance mode.<br>11. Removed Intel Virtualization Technology override when set to extreme performance (in extreme performance mode support only). |

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

***3.1 (5/3/2019)***

*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.  Set BMC MAC address to UUID for system without onboard LAN1 or with onboard LAN1 disabled.*
*8. Set PCIe correctable and uncorrectable (non-fatal) error report to disabled by default.*
*9. Set RFC4122 encoding to only be enabled for build time produced by IPMI 1.29 or newer.*
*10. Updated valid range of IPMI setup item VLAN ID to 1-4094.*
*11. Added driver health warning message.*
*12. Hid Driver Health page for SUM.*
*13. Reduced redundant reboot for offboard VGA switching.*
*14. Set NVDIMM ADR timeout to 600µs.*
*15. Enhanced the solution for the error/warning message from dmidecode after a modification by AMIDE.*
*16. Enhanced BIOS setup menu to auto-switch the Option ROM's value and hide the unexpected value when boot mode changes.*
*17. 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.*
*18. Fixed inability to change IPv6 address or IPv6 Router1 IP address.*
*19. Fixed problem of setup item "Quiet Boot" staying enabled after flashing BIOS with "Quiet Boot" disabled.*
*20. 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".*
*21. Modified UEFI network description to IPv4/IPv6 to follow Industry Standard.*
*22. 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).*
*23. Patched problem of system hanging at 0x94 when plugging in Nvidia Tesla T4 card.*
*24. Fixed failure to log memory UCE event due to incorrect flag.*
*25. Fixed inability of "Network Stack"-related items to get/change via SUM OOB method.*
*26. Fixed incorrect display of the TDP of Intel Speed Select table.*
*27. Patched problem of incorrect memory power being reported in PTU.*
*28. Applied workaround for inability of SUM to get full setting of IODC setup item.*
*29. Fixed loss of all LAN items when boot mode changes from Dual mode to UEFI mode.*
*30. Fixed failure to boot into VMware OS when set to Maximum Performance even if Monitor/MWAIT is enabled.*
*31. Temporarily fixed error for SKX (CLX) 4114 CPU memory training with Micron (18ASF2G72PDZ-2G6E1) RDIMM.*

***3.0a (1/12/2019)***

*1. Added support for Purley Refresh platform.*
*2. Updated SATA RAID OPROM/EFI driver to RSTe PreOS v6.0.0.1024.*
*3. Set BMC MAC address to UUID for system without onboard LAN1 or with onboard LAN1 disabled.*
*4. Set PCIe correctable and uncorrectable (non-fatal) error report to disabled by default.*
*5. Set RFC4122 encoding to only be enabled for build time produced by IPMI 1.29 or newer.*
*6. Updated CPU microcode SRV_P_264 for Skylake-SP H0/M0/U0 CPUs.*

*7. Disabled unused SPS ME "CUPS IIO" and "Volumetric Airflow" sensor.*
*8. Updated valid range of IPMI setup item VLAN ID to 1-4094.*
*9. Fixed problem of setup item "Quiet Boot" staying enabled after flashing BIOS with "Quiet Boot" disabled.*