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	**X12DPL-i6/NT6**
Release Version	**2.0**
Release Date	**02/07/2024**
Previous Version	**1.2**
Update Category	**Recommend**
Dependencies	**N/A**
Important Notes	**N/A**
Enhancements	**1. Update BIOS version to 2.0.** **2. Expose "Pre-boot DMA Protection".** **3. Apply SA50230 supplement (Image Parser Corruption Vulnerability).** **4. Apply SA50218 supplement (Vulnerability In EDK2 NetworkPkg).** **5. Update base to 5.22_WhitleyCrb_0ACMS_ICX_077.** **6. Update Intel Gigabit Lan driver to 9.8.09 (IBA 27.6).** **7. Fix system stuck at 0xB2 when plugging BPS with MM mode.** **8. Update SA50216_Supplement(LogoFAIL Vulnerability).** **9. Update base to 5.22_WhitleyCrb_0ACMS_ICX_077.** **10. Update Intel Gigabit Lan driver to 9.8.09 (IBA 27.6).** **11. Fix system stuck at 0xB2 when plugging BPS with MM mode.** **12. Update SA50216_Supplement(LogoFAIL Vulnerability).** **13. Update D/M stepping processor microcode to IPU 2023.4 out of band for Intel-TA-00950.** **14. Update 5.22_WhitleyCrb_0ACMS_ICX_076_BETA (IPU-PV 2023.3).** **15. Support VPD of card MCX562A-ACAB.** **16. Add SEL (Sensor Type : 0xC3, Data1 : 0x06, Data2 : CPU Index, Data3 : UPI Index) for UPI (topology change) link degraded.**

	17. Update secure boot DBX. 18. Update 5.22_WhitleyCrb_0ACMS_ICX_075 Intel 2023.2 IPU-PV. 19. Improve VROC key detection. 20. Boot option is not created for single hard drive under RAID mode. 21. Update 5.22_WhitleyCrb_0ACMS_ICX_74 (Intel BKC WW46 IPU2023.1). 22. Update Intel Server Platform Services for Whitley Server Platforms IPU2023.1 4.4.4.301. 23. Update SEL for processor error. 24. Update 5.22_WhitleyCrb_0ACMS_ICX_73 Intel BKCWW40 PLR3 OOB, please check header for firmware revisions. 25. Update VROC SATA/sSATA EFI driver to VROC PreOS v7.8.0.1012 to address 26. Moved AF w/a code. 27. Follow CPLD spec to set BIOS_EXIT_UBOOT and BIOS_BOOT_OK for VRM I2C protect 28. Follow the SMBIOS template sync the chassis type from FRU0 to SMBIOS Type 03. 29. Update 5.22_WhitleyCrb_0ACMS_ICX_72 Intel BKCWW23 PLR3, please check header for firmware revisions. 30. Update VROC SATA/sSATA EFI driver to VROC PreOS v7.7.6.1004 to adress INTEL-TA-00692. 31. Disable and expose "Link Retrain" in BIOS to avoid secondary Bus Reset following intel MOW. 32. If chassis type of FRU0 is not 1(other) or 2(unknown), sync it to SMBIOS type 3. 33. Add "CSM Support" setup item into SMCISBForm page.
New features	
Fixes	1. Fix HostInterface On/Off test will drop in 4x times in UEFI Shell.(Refer to EagleStream SVN3178) 2. Resolve KMS configuration can not be preserved after load BIOS default. 3. Display dynamic gateway IPV6 address as "::::::::" on BIOS setup if dynamic router info set count is 0. 4. Display static gateway IPV6 address as "::::::::" on BIOS setup if can not get valid gateway IPV6 address through IPMI. 5. Resolve TPM provision can not be done by SUM. 6. Fix incorrect total memory size on setup if install 6 memory.

	7. Fix memory is still mapped out because of UECC even after AC cycle. **8. Fix system halts after configure MMCFG Base to 1.5G and 1.75G.** **9. Fix ECO test case 2020 fails.** **10. Fixe memory error is not reported in SMBIOS event log.** **11. Enable all boot variable written back by Windows for test case 2071, 3056 and 4057.** **12. Resolve abnormal SOL resolution.**

1.2 (02/25/2022)

1. *Remove 1G option from MMCFG base to avoid system hang.*
2. *Fixed the SMBIOS event log ERROR CODE not display correctly under BIOS menu issue (EFI error type)*
3. *Correct "PCIe ASPM Support (Global)"" default value to disable*
4. *Rollback VROC SATA/sSATA EFI driver to VROC PreOS v7.6.0.1012 to fix system hang when VMD enable.*
5. *Fix COM port resource can't be changed and item's behavior fail.*
6. *Update AMI 5.22_WhitleyCrb_0ACMS_ICX_070_BETA RC27P52 for BKC 2021_WW52 (PLR1).*
7. *Change string "VMX" to "Intel Virtualization Technology"*
8. *Update 5.22_WhitleyCrb_0ACMS_ICX_069 Beta Intel BKCWW39 2021 PV MR7, please check header for firmware revisions.*
9. *Add flag [Preserve BIOS Boot Options Configuration] controlled by BMC/SUM.*

1.0b (09/03/2021)

1. *Update M87606A6_0D0002E0 microcode for Dx/Mx stepping CPU.*
2. *Update Intel BKCWW32 2021 PV MR5, please check header for firmware revisions.*
   [High] 14014151709 [ICX] Increase rrsr for channels that have roundtrip > 0x5a
   [High] 22013162072 SUT hungs while running Fisher tool command in RHEL OS
   [High] 14014133621,14014078778 BIOS should perform a global reset after EWL push and error harvesting when coming from a past warm reset boot CATERR/IERR
   [High] 22012792652 Memory - 3 Rank Memory 2 way Interleaving through ICX BIOS
   [High] 14014210150 System occurred iMC data parity error with MCACOD = 405 during stress
   [High] 14014144524 HSTI test fails for Secure Core Windows server
   [High] 18016147518 [ICX PCIE] Mask EB errors from being escalated to Receiver Error
   [High] 22012862056 [PCIe] BIOS to set sv.socket0.uncore.pcie.port0.dfx.pxpdllpctrl0.ack_period value to 0x1 before North PCIe training

[Medium] 1509144297 [ACM] Check SHA256 EVA_VALUE[00] & PCR_VALUE[00] value are different for add type 0x2E and changing size and updating IBB reset vector and Invalid KM header on BTGP0
[High] 1509142909 [ACM] After adding record type 0x2E and changing size and updating IBB reset vector and NO BPM on BTGP0, boot to BIOS failed
[Medium] 22011887647 [Core][ACM] Supporting Granular SCRTM for error conditions in CBnT
[High] 14014078016 ICX-SP disabled core X-prop resulting in MCA
[High] 18016118881 ICX PCIe SRIS Recipe Update
[High] 22012891374 20.P.88 MRC logs error when NVDIMM-Ns are installed
[High] 22012581859 Advanced Memtest code modification
[High] 1508927049 MSR_CRASHLOG_CONTROL_REGISTER definition for EnGprs bit is needed to enable GPR crashlog
[High] 22012608164 Semaphore mechanism fails once someone access(read) SYSTEMAQUSEMP[0] or SYSTEMAQUSEMP[1]
[High] 1508949647 System IERR after EfiPeiMemoryDiscovered when UEFI set chRankEnabled++ for DDRT
[High] 22012845839 Bad DIMM causes all BPS fail to be mapped to OS, also destroys BPS config
[High] 18015558621 Hit the issue of DXE_ASSERT urrentPollingState == 0 during NVIDMM AC cycling with 8+6 config
[High] 22012822697 [ICX][BPS][PV] Not able to create AD goal in 12+2 cfg
[High] 22012879848 [ICX][MSS][BPS] BIOS fix for 0 Margins in all Parameters in MRC flow
[High] 18016159697 Update Mgphy Recipe 3.8 to add Alternate Attentuator Table set values
[High] 18016487388 don't Sleep when NMTX mutex is held
[High] 22013000965,22013089757,22013327653 Enabling 256 PRMRR/Socket to enable SGX with mixed memory config
[High] 1509372838 OS hang during PI_RAS_einj_mem_uncorrectable_fatal test

1.0 (*04/06/2021*)

1. *First Release*