

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	X12DPT-PT6
Release Version	1.9
Release Date	01/05/2024
Previous Version	1.6
Update Category	Enhancement
Dependencies	None
Important Notes	None
Enhancements	<ol style="list-style-type: none">1. Update M87606A6_0D0003D1 microcode for Dx/Mx stepping CPU.2. Expose item Pre-boot DMA Protection.
New features	N/A
Fixes	<ol style="list-style-type: none">1. Update base to 5.22_WhitleyCrb_0ACMS_ICX_077 (2024.1 IPU-PV) for INTEL-SA-00960 Security Advisory to address CVE-2022-41804(6.1, Medium) security issue.2. Updated Intel Server Platform Services for Whitley Server Platforms IPU2024.1 4.4.4.603 for INTEL-SA-00960 Security Advisory to address CVE-2022-41804(6.1, Medium) security issue.3. Update AMITSE module for AMI SA50216 Security Advisory(LogoFAIL Vulnerability) to address CVE-2023-39538(7.5, High) and CVE-2023-39539(7.5, High) security issues.

Release Notes from Previous Release(s)

1.0 (05/25/2021)

Initial release.

1.1 (0708/2021)

1. Updated 5.22_WhitleyCrb_OACMS_ICX_066 Intel BKCWW24 2021 PV MR4.
2. Updated Dx/Mx microcode from Intel-Generic-Microcode-20210701_NDA.
3. Updated SATA/sSATA EFI driver to VROC PreOS v7.6.0.1012.

1.2 (02/14/2022)

1. Updated AMI 5.22_WhitleyCrb_OACMS_ICX_070_BETA RC27P52 for BKC 2021_WW52 (PLR1)
2. Updated Dx/Mx microcode from Intel-Generic-Microcode-20210927_NDA
3. Changed string "VMX" to "Intel Virtualization Technology".
4. Disabled EFI iSCSI support. (Refer Intel monthly BIOS/BMC review meeting - 7/22/2021)
5. Fixed SUM SMCKMS issues.
6. Fixed WHLK TPM 2.0 Supplemental test failure.
7. Fixed FW version and vendor in Trusted computing page.

1.4 (07/14/2022)

1. Update 5.22_WhitleyCrb_OACMS_ICX_72 Intel BKCWW23 PLR3
2. Update VROC SATA/sSATA EFI driver to VROC PreOS v7.7.6.1004 to address INTEL-TA-00692.Changed string "VMX" to "Intel Virtualization Technology".
3. Update BPS uEFI driver to 02.00.00.3886 for IPU2022.2.
4. Add "CSM Support" setup item into SMCISBForm page.

1.4b (01/17/2023)

1. Update 5.22_WhitleyCrb_OACMS_ICX_74 Intel BKCWW46 IPU2023
2. Update M87606A6_0D00037B microcode for Dx/Mx stepping CPU.
3. Update VROC SATA/sSATA EFI driver to VROC PreOS v7.8.0.1012 to address.
4. Update DBX file to fix Secure Boot Bypass issue.

1.6 (09/09/2023)

1. Updated Intel Server Platform Services for Whitley Server Platforms IPU2023.3 4.4.4.500
2. Update BMC/BMC Network Configuration page IPv6 DNS/DNS2 setting.
3. Change the strings from "Lock mode" to "Lockdown mode"

- | |
|--|
| <ol style="list-style-type: none">4. Fix incorrect total memory size on setup if install 6 memory.5. Fix memory still is mapped out because of UECC even after AC cycle. |
| |
| 1.9 (01/05/2024) <ol style="list-style-type: none">1. Update M87606A6_0D0003D1 microcode for Dx/Mx stepping CPU.2. Update base to 5.22_WhitleyCrb_0ACMS_ICX_077 (2024.1 IPU-PV) for INTEL-SA-00960 Security Advisory to address CVE-2022-41804(6.1, Medium) security issue.3. Updated Intel Server Platform Services for Whitley Server Platforms IPU2024.1 4.4.4.603 for INTEL-SA-00960 Security Advisory to address CVE-2022-41804(6.1, Medium) security issue.4. Update AMITSE module for AMI SA50216 Security Advisory (Logo FAIL Vulnerability) to address CVE-2023-39538(7.5, High) and CVE-2023-39539(7.5, High) security issues.5. Expose item Pre-boot DMA Protection. |