# BIOS Release Notes Form



| | |
|---|---|
| **Product Name** | **X12DPT-PT6** |
| **Release Version** | **2.1** |
| **Release Date** | **07/11/2024** |
| **Previous Version** | **1.9** |
| **Update Category** | **Enhancement** |
| **Dependencies** | **None** |
| **Important Notes** | **None** |
| **Enhancements** | 1. Update kernel to 5.22_WhitleyCrb_0ACMS_ICX_079 (2024.3 IPU).<br>2. Update Dx/Mx microcode for IPU2024.3 Security Advisory.<br>3. Apply AMI SA50235 for extended parser corruption correction.<br>4. Apply AMI SA50232 to address predictable TCP initial sequence numbers.<br>5. For SA50243 (CVSS3.1 (7.5, High)) fix that UsbRtSmm module has a TOCTOU vulnerability.<br>6. Patch for Mellanox InfiniBand Controller MAC Address issue.<br>7. Add third-party LAN card VPD support for AOC-E810-XXVDA4.<br>8. Update Aspeed_P2P_BUS and Aspeed_VGA_BUS settings to avoid system hang at PEI 0xA9. |
| **New features** | **N/A** |
| **Fixes** | **N/A** |

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

| |
|---|
| ***1.0 (05/25/2021)***<br>*Initial release.* |
| |
| ***1.1 (0708/2021)*** |

1. *Updated 5.22_WhitleyCrb_0ACMS_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_0ACMS_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_0ACMS_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_0ACMS_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
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)***

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.

***2.1 (07/11/2024)***

1. Update kernel to 5.22_WhitleyCrb_0ACMS_ICX_079 (2024.3 IPU).
2. Update Dx/Mx microcode for IPU2024.3 Security Advisory.
3. Apply AMI SA50235 for extended parser corruption correction.
4. Apply AMI SA50232 to address predictable TCP initial sequence numbers.
5. For SA50243 (CVSS3.1 (7.5, High)) fix that UsbRtSmm module has a TOCTOU vulnerability.
6. Patch for Mellanox InfiniBand Controller MAC Address issue.
7. Add third-party LAN card VPD support for AOC-E810-XXVDA4.
8. Update Aspeed_P2P_BUS and Aspeed_VGA_BUS settings to avoid system hang at PEI 0xA9.