

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	X12DPG-QT6
Release Version	2.1
Release Date	08/23/2024
Build Date	11/18/2024
Previous Version	2.0
Update Category	Critical
Dependencies	None
Important Notes	None
Enhancements	1.[Enhancements] Update kernel to 5.22_WhitleyCrb_0ACMS_ICX_079 (2024.3 IPU). 2.[Enhancements] Apply SA50235 for extended parser corruption correction. 3.[Enhancements] Support AOC-E810-XXVDA4. 4.[Enhancements] Apply AMI SA50232 to address predictable TCP initial sequence numbers. 1. CVE-2023-45236 Use of a Weak PseudoRandom Number Generator (Risk Level : 5.8). 2. CVE-2023-45237 Predictable TCP initial sequence numbers (ISNs) generated by the TCP/IP stack (Risk Level : 5.3). 6.[Enhancements] For SA50243 (CVSS3.1 (7.5, High)) fix that UsbRtSmm module has a TOCTOU vulnerability. 6.[Enhancements] Provide Mellanox InfiniBand mode MAC Address

	to SMBIOS type 40 structure. 8.[Fixes] Prevent system halt after enable Intel SGX.
New features	N/A
Fixes	1.[Fixes] Keep boot mode during IPMI force boot.

Release Notes from Previous Release(s)

2.0(02/01/2024)

- 1.[Enhancements] Update 5.22_WhitleyCrb_OACMS_ICX_075 Intel 2023.2 IPU-PV.
- 2.[Enhancements] Improve VROC key detection.
- 3.[Enhancements] Boot option is not created for single hard drive under RAID mode.
- 4.[Enhancements] Update 5.22_WhitleyCrb_OACMS_ICX_076_BETA (IPU-PV 2023.3).
- 5.[Enhancements] Update D/M stepping processor microcode to IPU 2023.4 out of band for Intel-TA-00950.
- 6.[Enhancements] Update base to 5.22_WhitleyCrb_OACMS_ICX_077 (2024.1 IPU-PV).
- 7.[Enhancements] Update secure boot KEK and DB.
- 8.[Enhancements] Expose "Pre-boot DMA Protection".
- 9.[Enhancements] Apply SA50216 supplement.
- 10.[Enhancements] Rebuild variable BootOrder according to previous boot if variable Boot0000 is created during OS installation.
- 11.[Enhancements] Apply SA50218 supplement (Vulnerability In EDK2 NetworkPkg / PixieFail VU#132380).
- 12.[Enhancements] Apply SA50230 supplement (Image Parser Corruption Vulnerability).
- 13.[Fixes] Fix system halts after configure MMCFG Base to 1.5G and 1.75G.
- 14.[Fixes] Fix ECO test case 2020 fails.
- 15.[Fixes] Resolve TPM provision can not be done by SUM.
- 16.[Fixes] Resolve system halts after install Intel Optane persistent memory.
- 17.[Fixes] Resolve KMS configuration can not be preserved after load BIOS default.

1.4b(02/24/2023)

- 1.[Enhancements] Update 5.22_WhitleyCrb_OACMS_ICX_74 (Intel BKC WW46 IPU2023.1).
- 2.[Enhancements] Update Intel Server Platform Services for Whitley Server Platforms IPU2023.1 4.4.4.301.
- 3.[Fixes] Fixe memory error is not reported in SMBIOS event log.
- 4.[Fixes] Enable all boot variable written back by Windows for test case 2071, 3056 and 4057.
- 5.[Fixes] Resolve abnormal SOL resolution.

1.4a(12/06/2022)

- 1.[Enhancements] Update 5.22_WhitleyCrb_OACMS_ICX_73 Intel BKCWW40 PLR3 OOB, please check header for firmware revisions.
- 2.[Enhancements] Update VROC SATA/sATA EFI driver to VROC PreOS v7.8.0.1012 to address Intel Virtual RAID on CPU (VROC): Data Loss Exposure Due to RAID 5 TRIM Support document #737276
- 3.[Enhancements] Moved AF w/a code.
- 4.[Enhancements] Follow CPLD spec to set BIOS_EXIT_UBOOT and BIOS_BOOT_OK for VRM I2C protect
- 5.[Enhancements] Follow the SMBIOS template sync the chassis type from FRU0 to SMBIOS Type 03.

6.[Fixes]Fix SOL resolution abnormal.

7.[Fixes]Fix SOL resolution abnormal.

1.4 (07/12/2022)

1.[Enhancements] Update 5.22_WhitleyCrb_OACMS_ICX_72 Intel BKCWW23 PLR3, please check header for firmware revisions.

2.[Enhancements] Update VROC SATA/sATA EFI driver to VROC PreOS v7.7.6.1004 to adress INTEL-TA-00692. CVE-2022-29919(7.8 High), CVE-2022-30338(6.7 Medium), CVE-2022-29508(6.3 Medium), CVE-2022-25976(5.5 Medium)

3.[Enhancements] Update 5.22_WhitleyCrb_OACMS_ICX_71 Intel BKCWW18 2022 PLR2, please check header for firmware revisions.

4.[Enhancements] Update BPS uEFI driver to 02.00.00.3886 for IPU2022.2.

5.[Enhancements] Add "CSM Support" setup item into SMCISBForm page.

6.[Enhancements] Filter Dynamic TCG Security Pages to patch SUM ChangeBiosCfg failed problem

7.[Enhancements] Update VROC SATA/sATA legacy driver to VROC PreOS v6.3.5.1003 Hot Fix to fix 10TB or higher volume drive issue.

8.[Enhancements] If chassis type of FRU0 is not 1(other) or 2(unknown), sync it to SMBIOS type 3.

1.2 (02/14/2022)

1.[Enhancements] Update AMI 5.22_WhitleyCrb_OACMS_ICX_070_BETA RC27P52 for BKC 2021_WW52 (PLR1)

2.[Enhancements]Change string "VMX" to "Intel Virtualization Technology".

3.[Fixes] Remove 1G option from MMCFG base to avoid system hang.

4.[Fixes] Fixed the SMBIOS event log ERROR CODE not display correctly under BIOS menu issue (EFI error type).

5.[Fixes] Correct "PCIe ASPM Support (Global)"" default value to disable.

6.[Fixes]Rollback VROC SATA/sATA EFI driver to VROC PreOS v7.6.0.1012 to fix system hang when VMD enable.

1.1 (04/09/2021)

1.[Enhancements] Updated BIOS ACM 1.0.9, SINIT ACM 1.0.9

2.[Enhancements] Updated SPS 4.4.4.53.

3.[Enhancements] Update SATA/sATA EFI driver to VROC PreOS v7.5.0.1152.

4.[Enhancements] The system cannot boot into PXE with DVD installed.

5.[Enhancements] Keep setup string of BiosVersion, BiosDate, Manufacturer and Product as default value including modification of AmiBcp.

6.[Enhancements] Add code to stop AFU support.

7.[Enhancements] Default enable BootGuard function.

8.[Enhancements] Extend memory DIMM serial number information.(Samsung, Micron, Hynix)

9.[Enhancements] Enhance Smc Dcpmm feature.

10.[Enhancements] Automatically disable and grayed out ADDDC, UMA-Base Clustering, mirror mode and enable NUMA when SGX enabled.

11.[Enhancements] Remove intel lan memory 4G limit if boot mode is not legacy.

12.[Enhancements] Set all oprom control items to Legacy when boot mode set to Dual.

13.[Enhancements] Update for 20P95_LB62_PreDrop_V1 for BKC WW15 (20P95)

14.[Enhancements] Update Intel-Generic-Microcode-20210226a_NDA and Intel AE (updated)

15.[Fixes] Fix "Configuration Address Source" always show "DHCP" in IPMI IPv6 page.

16.[Fixes] Fix Memory correct error location is wrong in BIOS event log for CPU2.

17.[Fixes] Modify Ipv6 behavior, remove error message when Ipv6 router IP is :::::

18.[Fixes] Correct CPU1 memory type 20 handler point to CPU2 Memory Array Mapped Address structure

- 19.*[Fixes] Fix IPv6 Status show incorrect after updating BIOS.*
- 20.*[Fixes] Fixed IPv4 address source status show incorrect after updating BIOS issue.*
- 21.*[Fixes] Fixed the HDD security menu will not show when connect more than 6 HDD on system.*
- 22.*[Fixes] Fix IPV6 disable in the IPMI GUI but BIOS initialize will appear IPV6 address..*
- 23.*[Fixes] Filter Dynamic HDD Security Pages to patch SUM ChangeBiosCfg failed problem.*
- 24.*[Fixes] Fixed UEFI OS boot option name shows incorrectly in BIOS setup.*
- 25.*[Fixes] Fix T-states always show 15 levels even T-state is disabled.*

1.0 (12/02/2020)

- 1. *First Release.*