BIOS Release Notes Form

Product Name	**X12DPG-U6**
Release Version	**1.9**
Release Date	**3/15/2024**
Build Date	**1/2/2024**
Previous Version	**1.6**
Update Category	**Critical**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1.[Enhancements] Update Dx/Mx BETA microcode for IPU2023.4 Out of band for Intel-TA-00950** **2.[Enhancements] Update BIOS version to 1.9.** **3.[Enhancements] Update M87606A6_0D0003D1 microcode for Dx/Mx stepping CPU. For INTEL-SA-00950 Security Advisory to address CVE-2023-23583(8.8, High) security issue. For INTEL-SA-00960 Security Advisory to address CVE-2022-41804(6.1, Medium)security issue.** **4.[Enhancements] 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.** **5.[Enhancements] 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.**

	6.[Enhancements] Apply AMI LogoFAIL Vulnerability Supplement for SA50216 Security Advisory to address CVE-2023-39539(7.5, High) security issue.
New features	None
Fixes	None

Release Notes from Previous Release(s)

1.6(6/16/2023)
1.[Enhancements] Update BIOS version to 1.5.
2.[Enhancements] Update 5.22_WhitleyCrb_0ACMS_ICX_075 Intel 2023.2 IPU-PV, please check header for firmware revisions.
3.[Enhancements] Pull high GPP_C10_FM_PCH_SATA_RAID_KEY first before VROC key detection
4.[Enhancements] Update BIOS version to 1.6.
5.[Enhancements] Update 5.22_WhitleyCrb_0ACMS_ICX_076_BETA (IPU-PV 2023.3).
6.[Enhancements] Update M87606A6_0D0003A5 microcode for Dx stepping CPU.
7.[Enhancements] Updated SPS 4.4.4.500.
8.[Enhancements] Update VROC SATA/sSATA EFI driver to VROC PreOS v8.0.0.4006 .
9.[Enhancements] Change the strings from "Lock mode" to "Lockdown mode".

1.4b(4/10/2023)
1. [Enhancements] Update BIOS version to 1.4b.
2. [Enhancements] Update 5.22_WhitleyCrb_0ACMS_ICX_74 Intel BKCWW46 IPU2023.1, please check header for firmware revisions.
3. [Enhancements] Updated Intel Server Platform Services for Whitley Server Platforms IPU2023.1 4.4.4.301

1.4a(01/18/2023)
1.[Enhancements] Update BIOS version to 1.4a.
2.[Enhancements] Update 5.22_WhitleyCrb_0ACMS_ICX_73 Intel BKCWW40 PLR3 OOB, please check header for firmware
revisions. For INTEL-SA-00657 Security Advisory to address CVE-2022-21233(6.0, Medium) security issue. For INTEL-SA-00686
Security Advisory to address CVE-2021-33060(7.8, High) security issue.
3.[Enhancements] a) Update VROC SATA/sSATA EFI driver to VROC PreOS v7.8.0.1012 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) b) Update
VROC SATA/sSATA 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 c) Update VROC SATA/sSATA legacy driver to VROC PreOS v6.3.5.1003 Hot
Fix to fix 10TB or higher volume drive issue.
4.[Enhancements] Update ucode M87606A6_0D00037B to address below issue. For INTEL-SA-00657 Security Advisory to

address CVE-2022-21233(6.0, Medium) security issue. For INTEL-SA-00686 Security Advisory to address CVE-2021-33060(7.8,

High) security issue.

5.[Enhancements] Update BPS uEFI driver to 02.00.00.3887 for IPU2022.3.

6.[Enhancements] Update DBX file to fix Secure Boot Bypass issue.

7.[Enhancements] Follow the SMBIOS template sync the chassis type from FRU0 to SMBIOS Type 03.

8.[Enhancements]Follow CPLD spec to set BIOS_EXIT_UBOOT and BIOS_BOOT_OK for VRM I2C protect

1.4 (07/07/2022)

1.[Enhancements] Update BIOS version to 1.4.

2..[Enhancements] Update 5.22_WhitleyCrb_0ACMS_ICX_72 Intel BKCWW23 PLR3, please check header for firmware revisions. For INTEL-SA-00657 Security Advisory to address CVE-2022-21233(6.0, Medium) security issue. For INTEL-SA-00686 Security Advisory to address CVE-2021-33060(7.8, High) security issue.

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

5.[Enhancements] Update SINIT ACM 1.1.0 and BIOS ACM 1.1.0.

6.[Enhancements] Update ucode M876CPLD06A6_0D000375 to address below issue. For INTEL-SA-00657 Security Advisory to address CVE-2022-21233(6.0, Medium) security issue. For INTEL-SA-00686 Security Advisory to address CVE-2021-33060(7.8, High) security issue.

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

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

9.[Enhancements] Disable Link Re-train in BIOS to avoid secondary Bus Reset following intel MOW 22WW27 and expose Link Re-train per port in BIOS.

1.2 (03/07/2022)

1.[Enhancements] Update AMI 5.22_WhitleyCrb_0ACMS_ICX_070_BETA RC27P52 for BKC 2021_WW52 (PLR1)

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

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

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

5.[Fixes] Fix SpeedStep (P-States) setting change when its default setting is set to Disable and load BIOS defaults in Setup.

6.[Enhancements] Update Dx/Mx microcode from Intel-Generic-Microcode-20210927_NDA.

7.[Enhancements] Update SINIT ACM 1.0.F and BIOS ACM 1.0.E.

8.[Fixes] Fix the problem of x-AMI test failure in SmcKMS related items.

9.[Fixes] Added "Preserve_SMBIOS", "Preserve_OA" into FlashFlag when in the condition "NvramDefaultMode".

10.[Fixes] a) Rollback VROC SATA/sSATA EFI driver to VROC PreOS v7.6.0.1012 to fix system hang when VMD enable. b) Update VROC SATA/sSATA legacy driver to VROC PreOS v6.3.5.1003

11.[Fixes] Fixed issue that the OPROM control item of the riser card " RSC-H2-68G4" cannot expose in the BIOS setup menu when the system installs the AOC card "AOC-S25GC-I2S".

12.[Fixes] Fixed issue that the tests fail with the SUM ECO test cases 287 and 288 when the system connect to the Habana carrier board.

1.0b (09/07/2021)

1.[Enhancements] Disable EFI iSCSI support. (Refer Intel monthly BIOS/BMC review meeting - 7/22/2021)

2.[Enhancements] Patch BMC Redfish Host Interface was named as ethX when CDN was disabled case under Linux OS.
3.[Enhancements] Update BIOS version to 1.1b.
4.[Enhancements] Update 5.22_WhitleyCrb_0ACMS_ICX_067 Intel BKCWW32 2021 PV MR5, please check header for
firmware revisions.
5.[Enhancements] Update Dx/Mx microcode from Intel-Generic-Microcode-20210804_NDA.
6.[Enhancements] Update BIOS/SINIT ACM 1.0.D.
7.[Enhancements] Updated SPS 4.4.4.58.
8.[Enhancements] Add flag [Preserve BIOS Boot Options Configuration] controlled by BMC/SUM
9.[Fixes] Add a path to check the OAM devices speed/width drop.

1.0a (06/11/2021)
1.[Enhancements] [X12DPG-U6] Change revision to 1.0a.
2.[Enhancements] Update 5.22_WhitleyCrb_0ACMS_ICX_065_BETA for Intel BKCWW20 2021 PV MR3.
3.[Enhancements] Update Dx/Mx microcode from Intel-Generic-Microcode-20210528_NDA.
4.[Enhancements] Updated SPS 4.4.4.56.
5.[Enhancements] Updated BIOS ACM 1.0.A, SINIT ACM 1.0.A.
6.[Enhancements] Update SATA/sSATA EFI driver to VROC PreOS v7.6.0.1012.
7.[Fixes] Fix SGX settings can't be preserve after updating BIOS. The function can't support IPMI web updating BIOS.
8.[Fixes] Fixed the AER issue of the carrier board.

1.0 (04/07/2021)
1.   First Release.