BIOS Release Notes Form

Product Name	**X12DPU-6**
Release Version	**2.3 SPS: 4.4.4.702**
Build Date	**03/29/2025**
Previous Version	**2.2 SPS: 4.4.4.702**
Update Category	**Recommended**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Updated kernel to 5.22_WhitleyCrb_0ACMS_ICX_082 (IPU 2025.2 PV).** **2. Applied SA50300 to address the CVE-2024-7344 (High, 8.2) security issue.** **3. Removed the warning message, "Crystal Ridge is not support."** **4. Applied AMI SA50288 to address OpenSSL MbedTLS (CVE-2023-52353) and Elliptic Curve API (CVE-2024-9143) vulnerabilities.** **5. When enabling block SID, set AUTO_ACCEPT_PPI to avoid having to wait for user acceptance to continue.** **6. Avoid loading multiple video cards since it can result in system hang or no video display.** **7. Updated Intel boot agent 30.0 for Giga and 10 G uEFI driver.**

New features	**None**
Fixes	**1. If HTTP boot was ever configured on BIOS setup or via SUM, skip the boot order update.** **2. Resolved how the off-board VGA graphics output protocol was still installed as "VGA Priority" is "Onboard."** **3. Updated the boot order by UEFI/legacy/dual boot category and boot option sequence to reflect HW configuration before referring to it.** **4. Fixed how the built-in UEFI shell resulted in no mapping found after enabling Legacy to EFI support and set boot mode to Dual mode.**

Release Notes from Previous Release(s)

2.2 SPS: 4.4.4.702 (10/24/2024)

1. *Updated kernel to 5.22_WhitleyCrb_0ACMS_ICX_081 (2025.1 IPU PV).*
2. *Applied SA50230 supplement (Image Parser Corruption Vulnerability).*
3. *Applied SA50218 supplement (Vulnerability In EDK2 NetworkPkg).*
4. *For SA50243 (CVSS3.1 (7.5, High)), fixed how the UsbRtSmm module had a TOCTOU vulnerability.*
5. *Applied SA50235 for extended parser corruption correction.*
6. *Applied AMI SA50232 to address the security vulnerability listed below.*
    a. *CVE-2023-45236 Use of a Weak PseudoRandom Number Generator (Risk Level : 5.8).*
    b. *CVE-2023-45237 Predictable TCP initial sequence numbers (ISNs) generated by the TCP/IP stack (Risk Level : 5.3).*
7. *Enhanced ErstWriteErrorRecord () and ErstReadErrorRecord () for security vulnerabilities (Refer to EagleStream SVN 3722).*
8. *Set Chassis type in smbios to default (0x11) when the Chassis type from fru was 0x00 or 0xFF.*
9. *Saved MAC to PCD for filling DUID with UUID (Refer to EagleStream SVN 3621 and 3622).*
10. *SMBIOS type 40 VPD update.*
11. *Exposed PCI-E Completion Timeout.*
12. *Removed the VLAN callback function in Setup BMC page.*
13. *Removed setup callback relative to BMC Network Configuration (Refer to EagleStream SVN 3833).*
14. *Runtime updated the smbios date to ROMHOLE (Refer to EagleStream SVN 3839).*
15. *Resolved IPMI PXE boot fails after installing OS.*
16. *Resolved how the boot order could not be adjusted by AMI SCE.*
17. *Overwrote AmiPcdChassisType to sync SYS_CHASSIS_TYPE_1 setting.*
18. *Kept boot mode during IPMI force boot.*
19. *Fixed the no copyright string in text mode.*

1.9 SPS: 4.4.4.603 (01/11/2024)

1. *Updated the 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.*
2. *Exposed "Pre-boot DMA Protection."*
3. *Applied SA50216 supplement.*
4. *Resolved how the KMS configuration could not be preserved after load BIOS default.*
5. *Fixed how the HostInterface On/Off test will drop four times in UEFI Shell. (Refer to EagleStream SVN3178.)*
6. *Resolved how the CPU2 TDP on BMC WebUI displayed 0 sometimes.*
7. *Displayed dynamic gateway IPV6 address as "::::::" on a BIOS setup if the dynamic router info set count was 0.*
8. *Displayed static gateway IPV6 address as "::::::" on a BIOS setup if it could not get a valid gateway IPV6 address through IPMI.*

1.8 SPS: 4.4.4.603 (11/22/2023)

1. *Updated base to 5.22_WhitleyCrb_0ACMS_ICX_077.*
2. *Updated Dx/Mx PC microcode Intel-Restricted-2024-1-IPU-20231009_20241IPU for IPU2024.1.*
3. *Fixed the system stuck at 0xB2 when plugging BPS with MM mode.*
4. *Added mapping language for SGX related items.*
5. *Updated Intel Server Platform Services for Whitley Server Platforms IPU2024.1 4.4.4.603.*

1.6 SPS: 4.4.4.500

1. *Updated BIOS revision to 1.6.*
2. *Updated 5.22_WhitleyCrb_0ACMS_ICX_076_BETA (IPU-PV 2023.3).*
3. *Change the strings from "Lock mode" to "Lockdown mode".*
4. *Removed duplicated "ENERGY_PERF_BIAS_CFG Mode" HII data.*

1.5 SPS: 4.4.4.301 (4/26/2023)

1. *[Enhancements] Updated 5.22_WhitleyCrb_0ACMS_ICX_74 Intel BKCWW46 for IPU2023.1.*
2. *[Enhancements] Fine-tuned VROC key detection function.*

1.4b SPS: 4.4.4.301 (1/13/2023)

1. *Updated 5.22_WhitleyCrb_0ACMS_ICX_74 Intel BKCWW46 for IPU2023.1; please check header for firmware revisions.*
2. *Added enhancements when running the SUM TC: 220/271/356/457/2071/3056/4057 with Windows OS will cause the boot order to compare fail after flashing the BIOS.*
3. *Changed BIOS revision to 1.4b.*

1.4a (11/24/2022)

1. *Updated 5.22_WhitleyCrb_0ACMS_ICX_73 Intel BKCWW40 PLR3 OOB, please check the header for firmware revisions.*
2. *Updated 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)*
3. *Followed CPLD spec to set BIOS_EXIT_UBOOT and BIOS_BOOT_OK for VRM I2C protect.*
4. *Followed the SMBIOS template sync the chassis type from FRU0 to SMBIOS Type 03.*
5. *Updated Intel Server Platform Services for Whitley Server Platforms.*
6. *Fixed system, will not attempt Legacy PXE boot, even set network to first priority when there is other legacy OS on the system issue.*

1.4 (7/12/2022)

1. *Updated 5.22_WhitleyCrb_0ACMS_ICX_72 Intel BKC WW23 PLR3.*
2. *Updated 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).*
3. *Updated VROC SATA/sSATA legacy driver to VROC PreOS v6.3.5.1003 Hot Fix to fix 10TB or higher volume drive issue.*
4. *Added "CSM Support" setup item into SMCISBForm page.*
5. *Fixed Dynamic TCG Security Pages to patch SUM ChangeBiosCfg failure problem. SUM cannot parse dynamic pages that only update form when enter bios setup menu.*
6. *Added support for IPMI PXE boot to all LAN port feature for both Legacy and UEFI PXE. When using the IPMI system boot option command to boot to Legacy PXE or UEFI PXE, the system should scan all LAN ports.*
7. *Fixed Linux OS showing incorrect CPU max freq. Customer reported the PLR1 BIOS showing the wrong CPU max speed while previous BIOS does not have such issue.*
8. *[SmcOOB]: Updated SmcOOB to the version "_SMCOOBV1.01.25_" to fix the unexpected system-reseting when loading NVRAM defaults. Updated SmcOOB to the version "_SMCOOBV1.01.25_" to fix the unexpected system-resetting when loading the BIOS default.*

9. *If chassis type of FRU0 is not 1(other) or 2(unknown), sync it to SMBIOS type 3. SMBIOS template rule update*
10. *Disable Link Re-train in BIOS to avoid secondary Bus Reset following intel MOW 22WW27 and expose Link Re-train per port in BIOS.*
11. *Fixed SUM ChangeBiosCfg command which cannot update PchSetup variable related BIOS items. BIOS settings such as "Configure SATA should be able to be updated by SUM (Supermicro Update Manager).*

1.2 (2/15/2022)

1. Changed BIOS revision to 1.2.
2. Updated PLR1 HF RC27P56, ucode M87606A6_0D000332.
3. Changed string "VMX" to "Intel Virtualization Technology".
4. Added flag [Preserve BIOS Boot Options Configuration] controlled by BMC/SUM.
5. Updated AMI 5.22_WhitleyCrb_0ACMS_ICX_070_BETA RC27P52 for BKC 2021_WW52 (PLR1).
5. Removed 1G option from MMCFG base to avoid system hang.
6. Fixed the SMBIOS event log ERROR CODE, which did not display correctly under BIOS menu (EFI error type).
7. Fixed COM port resource that can't be changed, item behavior failure.
8. Fixed the IIO menu of onboard P1_NVMe1 slot, it does not show under BIOS menu.

1.1a (8/21/2021)

1. Updated 5.22_WhitleyCrb_0ACMS_ICX_067 Intel BKCWW32 2021 PV MR5.
2. Updated Dx/Mx microcode from Intel-Generic-Microcode-20210804_NDA.
3. Updated SPS 4.4.4.58 PV MR5.
4. Changed BIOS revision to 1.1a.
5. Changed "Hard Drive Security Frozen" default setting to disabled.
6. Disabled support for EFI iSCSI.
7. Added support for SUM upload/delete HTTPS TLS certificate.
8. Set absence of onboard LAN to be reported to BMC when there is no onboard LAN on system.
9. Fixed failure of SUM TC 221 when installing multiple NICs on system.

1.1 (4/21/2021)

1. Updated RC 20.P95 for PV RC update.
2. Changed the BIOS version to 1.1.
3. Updated for CPLD Signature table 101.
4. Updated Intel-Generic-Microcode-20210402_NDA.
5. Updated Dx/Mx microcode from Intel AE (synced with BKCWW14).

1.0b (3/26/2021)

1. Updated RC 20.P93 for PV RC update.
2. Updated BIOS ACM 1.0.9 and SINIT ACM 1.0.9.
3. Updated SPS 4.4.53.
4. Updated x/Mx microcode from Intel AE.

5. Automatically disabled and hid ADDDC with x8 width DIMM.
6. Extended memory DIMM serial number information (Samsung, Micron, Hynix).
7. Enhanced SMC DCPMM feature.
8. Automatically disabled and grayed out ADDDC, UMA-Base Clustering, and mirror mode and enabled NUMA when SGX is enabled.
9. Set relation setup to restore setting after "Factory Mode" is disabled.
10. Removed 4G limit of Intel LAN memory if boot mode is not legacy.
11. Set all OPROM control items to Legacy when boot mode is set to Dual.
12. Updated SATA/sSATA EFI driver to VROC PreOS v7.5.0.1152.
13. Updated BPS firmware to 2.2.0.1553.
14. Changed the BIOS version to 1.0b.
15. Fixed problem of T-states always showing 15 levels even when T-state is disabled.
16. Filtered Dynamic HDD Security pages to patch failure of SUM ChangeBiosCfg.
17. Fixed inability to upload all OOB files on the first BMC boot.
18. Corrected display of UEFI OS boot option name in BIOS setup.
19. Corrected riser card SMBIOS creation.
20. Fixed problem with a CPU exception.
21. Fixed failure to hide the SmcSecureErase setup page when no HDD devices are plugged in.
22. Corrected display of NVMe LED on BPN-NVMe4-216N-S24 under VMD mode.

1.0a (1/28/2021)

1. Changed the BIOS version to 1.0a.
2. Updated BKC WW51 components.
3. Fixed inability of system to boot into PXE with DVD installed.
4. Fine tuned re-timer add-on card workaround.
5. Fixed problem of system exception occurring at 0x92 or 0xA2 after changing boot order and rebooting.
6. Corrected CPU1 memory type 20 handler point to CPU2 Memory Array Mapped Address structure.
7. Fixed failure of the HDD security menu to display when connecting more than 6 HDDs on system.

1.0 (10/22/2020)

1. First release

_____ _____

Product Manager *Date*