BIOS Release Notes Form

Product Name	**X12DPFR-AN6**
Release Version	**2.3 SPS: 4.4.4.702**
Build Date	**03/29/2025**
Previous Version	**1.8 SPS: 4.4.4.603**
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. Remove 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. Avoided loading multiple video cards since it could cause system hang or result in 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, skipped the boot order update.** **2. Update boot order by UEFI/legacy/dual boot category and boot option sequence to reflect HW configuration before referring to it.** **3. Fixed how the built-in UEFI shell resulted in no mapping found after enabling Legacy to EFI support and setting boot mode to Dual mode.** **4. Fine-tuned NVMe VMD code.**

Release Notes from Previous Release(s)

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 system stuck at 0xB2 when plugging BPS with MM mode.*
4. *Updated Intel Server Platform Services for Whitley Server Platforms IPU2024.1 4.4.4.603.*

1.5 SPS: 4.4.4.301 (4/26/2023)

1. *Added ECM RNDIS support.*
2. *No boot option for single HDD under RAID mode.*
3. *Fine-tuned VROC key detection function.*
4. *Updated BIOS revision to 1.5.*
5. *Updated 5.22_WhitleyCrb_0ACMS_ICX_075 Intel 2023.2 IPU-PV.*
6. *Pulled high GPP_C10_FM_PCH_SATA_RAID_KEY first before VROC key detection.*
7. *Fixed system hangs on 0xA9 after setting MMCFG base to 1.5G and 1.75G.*
8. *Fixed that the SUM TC: 2020 test fail problem.*

1.4b (1/12/2023)

1. *Updated 5.22_WhitleyCrb_0ACMS_ICX_74 Intel BKCWW46 IPU2023.1, please check header for firmware revisions.*
2. *Updated Intel Server Platform Services for Whitley Server Platforms IPU2023.1 4.4.4.301.*

3. *Updated VROC SATA/sSATA EFI driver to VROC PreOS v7.8.0.1012.*
4. *Fixed an issue where memory errors were not being reported in the SMBIOS event log.*

1.2 (3/16/2022)

1. *Changed string "VMX" to "Intel Virtualization Technology".*
2. *Added flag [Preserve BIOS Boot Options Configuration] controlled by BMC/SUM.*
3. *Changed BIOS revision to 1.2*
4. *Updated VROC SATA/sSATA legacy driver to VROC PreOS v6.3.5.1003 Hot Fix to fix 10TB or higher volume drive issue.*
5. *Enhanced get VPD data routines for E810.*
6. *Fine tuned the delay time for get VPD data routines.*
7. *Updated AMI 5.22_WhitleyCrb_0ACMS_ICX_070 RC27P56 for BKC 2021_WW52 (PLR1 HF)*
8. *Removed 1G option from MMCFG base to avoid system hang.*
9. *Fixed the SMBIOS event log ERROR CODE, it is not displaying correctly under BIOS menu issue (EFI error type).*
10. *Fixed SpeedStep (P-States) setting, changed when its default setting is set to Disable, and load BIOS defaults in Setup.*
11. *Fixed COM port resource that can't be changed, and item's behavior failure.*

1.1b (11/20/2021)

1. Updated 5.22_WhitleyCrb_0ACMS_ICX_069 Intel BKCWW39 2021 PV MR7
2. Updated Dx/Mx microcode from Intel-Generic-Microcode-20210927_NDA.
3. Disabled EFI iSCSI support.
4. Enhanced DMI type 42 to support EUI-48.
5. Now supports EUI-48 Locally Administered MAC Addresses.
6. Turned on Shutdown Suppression and Log MCA IERR to fix crash dump error.
7. Changed the default setting of PPR from "Enabled" to "Disabled".
8. Changed string "VMX" to "Intel Virtualization Technology".
9. Fixed issue where COM port resource can't be changed, and item's function fails.
10. Fixed clear bits of IPMI CMD 30_A0_15 according to usage of location instead of all bytes.
11. Fixed the SMBIOS event log ERROR CODE not displaying correctly under BIOS menu issue (EFI error type).
12. The grayed-out setup item "Lockdown Mode" has been fixed.
13. Fixed MMCFG base system hang issue.

***1.1a (9/1/202*1)**

12. *Updated 5.22_WhitleyCrb_0ACMS_ICX_067 Intel BKCWW32 2021 PV MR5.*
13. *Updated Dx/Mx microcode from Intel-Generic-Microcode-20210804_NDA.*
14. *Updated SmcOOB module to 1.01.24 to support SUM clean SMBIOS Event log through BiosCfg header flag.*
15. *Updated riser card string on SMBIOS type 9.*
16. *Set default Boot Guard profile to 5.*
17. *Updated ASPEED VBIOS and EFI driver to 1.11.03.*
18. *Kept value of setup string of Manufacturer and Product according to priority "modification of AmiBcp, FRU1, and then SMBIOS Table".*
19. *Added code to stop AFU support.*
20. *Added HCC Mx stepping CPU check for CPU stepping display.*

21. *Automatically disabled and hid ADDDC with x8 width DIMM.*
22. *Removed 4G limit of Intel LAN memory if boot mode is not legacy.*
23. *Automatically disabled and grayed out ADDDC, UMA-Base Clustering, and mirror mode and enabled NUMA when SGX is enabled.*
24. *Enhanced SMCI HDD Security feature.*
25. *Extended memory DIMM serial number information (Samsung, Micron, Hynix).*
26. *Enhanced SMC DCPMM feature.*
27. *Set all OPROM control items to Legacy when boot mode is set to Dual.*
28. *Updated CPLD Signature table 101 and tool to 1.30.24 for CPLD Signature.*
29. *Corrected the length of riser card string dynamic update for SMBIOS type 9 slot.*
30. *Escalated UNCA error.*
31. *Modified Me version strings and removed the "Manufacturer ID" string.*
32. *Corrected firmware version and vendor on Trusted Computing page.*
33. *Corrected display of IPv4 address source status after updating BIOS.*
34. *Corrected location of RT UECC log.*
35. *Fixed failure of RT UECC to be mapped out.*
36. *Enabled unprogrammed AOC to be plugged in without causing endless restarts.*
37. *Corrected display of IPv6 when IPv6 status is not active.*
38. *Filtered Dynamic HDD Security pages to patch failure of SUM ChangeBiosCfg.*
39. *Fixed problem of T-states always showing 15 levels even when T-state is disabled.*
40. *Fixed problem with a CPU exception.*
41. *Fixed failure to hide the SmcSecureErase setup page when no HDD devices are plugged in.*
42. *Corrected display of UEFI OS boot option name in BIOS setup.*
43. *Fixed failure of Secure Boot Append/Update Keys.*
44. *Fixed inability to upload all OOB files on the first BMC boot.*
45. *Corrected memory device number in SMBIOS type 16.*
46. *Corrected iSCSI Configuration page.*
47. *Set DIMM size to recalibrate when rank is disabled.*
48. *Updated non-VPD Intel MAC report routine for 64bit BAR.*