IPMI Firmware / BIOS Release Notes Form

Product Name	**X11DPT-B(H)**
Release Version	**2.1a**
Release Date	**9/15/2018**
Previous Version	**2.1**
Update Category	**Recommended**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Set PCIe link status to be polled at DXE stage to fix wrong information in BIOS setup IIO page.** **2. Disabled "tRWSR Relaxation" by default.** **3. Added support for Monitor Mwait feature.** **4. Updated SPS 4.0.4.381 for INTEL-SA-00131 Security Advisory to address CVE-2018-3643 and CVE-2018-3644 security issues.** **5. Fixed inability of VMD status to load default if loading default by AFU.** **6. Updated CPU microcode SRV_P_253 for Skylake-SP H0/M0/U0 stepping CPUs.**
New features	**N/A**

Fixes	1. Fixed missing sensor reading for add-on devices.
	2. Fixed problem of BIOS always retrying boot when Re-Try Boot is Disabled.
	3. Fixed malfunction of BIOS/ME downgrade check when running flash package (SWJPME2) a second time.
	4. Fixed problem of system resetting while flashing BIOS under OS if Watch Dog function is enabled.
	5. Fixed missing information for Hybrid backplane SMBIOS type 39.
	6. Fixed failure of turbo in new Linux kernel.

2.1 (7/13/2018)

1. Updated CPU microcode to address 'Spectre' derivatives (CVE-2018-3639 & CVE-2018-3640) security issue.
2. Updated 5.12_PurleyCrb_0ACFD088 for Purley Skylake platform PLR7, BKC 2018 WW20.
3. Updated Giga LAN EFI driver 8.3.0.4 (IBA 23.1).
4. Updated SPS 4.00.04.340 PV PLR7 version.
5. Updated SATA RAID OPROM/EFI driver to RSTe PreOS v5.4.0.1039.
6. Corrected default setting for Enable SmcBusMasterEn setup item.
7. Corrected BIOS/ME downgrade check for SPS 4.0.4.340.
8. Added support for UEFI mode PXE boot of F12 hot key Net boot.
9. Added one event log to record that the event log is full.
10. Updated BIOS ACM 1.3.7 and SINIT ACM 1.3.4.
11. Fixed problem of SUM GetSataInfo showing incorrect "Configuration Type" when setting "Configure sSATA as" to "AHCI" or "RAID" on sSATA controller.
12. Fixed problem of Ctrl + Alt + Del causing system to hang after flashing BIOS.
13. Fixed missing NVDIMM ADR setup item.
14. Fixed problem of system hanging when installing Linux OS after COM1 & COM2 IO/IRQ exchange.

2.0b (2/24/2018)

1. Updated CPU microcode to address CVE-2017-5715 security patch issue.
2. Updated 5.12_PurleyCrb_0ACFD085Beta for Purley Skylake platform PLR 4, BKC WW02.
3. Added setup item "SmcBusMasterEn" for enabling Parent bridge of the devices in the gSmcPciForceEnableBusMasterList.
4. Changed RC default setting to upgrade POST Memory correctable error to uncorrectable error and map out the channel.
5. Added support for System Firmware Progress System Firmware Progress feature.
6. Fixed inability to reset the system under DOS by pressing "Ctrl-Alt-Del" on USB keyboard when "Port 60/64 Emulation" is disabled.
7. Fixed problem of SMC skipping first boot option in UEFI mode when retrying boot.
8. Fixed malfunction of "SMBIOS Preservation" Disabled.
9. Fixed issue of all commands requesting to be persistent.
10. Disabled CPU2 IIO PCIe root port ACPI hot plug function.
11. Fixed issue with IPMI force boot.
12. Fixed malfunction of option ROM control for AOC-MTG-i2TM and BPN-ADP-12NVMe-2UB.
13. Fixed problem of system hanging during BIOS flashing if Watch Dog function is enabled.
14. Fixed problem of the system not logging memory errors upon injection without rebooting.
15. Fixed incorrect LED behavior if VMD is disabled by stack but not by ports.