IPMI Firmware / BIOS Release Notes Form

Product Name	**X11DPT-PS**
Release Version	**2.1**
Release Date	**8/23/2018**
Previous Version	**2.0b**
Update Category	**Recommended**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Updated CPU microcode to address 'Spectre' derivatives (CVE-2018-3639 & CVE-2018-3640) security issue.** **2. Changed BIOS revision to 2.1.** **3. Updated Giga LAN EFI driver 8.3.0.4 (IBA 23.1).** **4. Added 1T option for MMIO High Base setup item.** **5. Added BIOS/ME downgrade check for SPS 4.0.4.381.** **6. Changed maximum speed in SMBIOS type 4 to 4500Mhz.** **7. Added one event log to record that the event log is full.** **8. Added support for SATA FLR.** **9. Displayed PPR setup item.** **10. Added a patch to prevent reboot hang when installing AVAL APX-3224 card.** **11. Moved SIOM SMBIOS definition from type 41 to type 9.** **12. Exported driver health menu under setup.**

	13. Added support for full function of AOC-MHIBE-M1CGM SIOM.
New features	**N/A**
Fixes	**1. Fixed problem of Ctrl + Alt + Del causing system to hang after flashing BIOS.** **2. Fixed problem of some NVDIMM items not appearing in setup menu.** **3. Fixed incorrect VPD data and oversized string to prevent system from hanging.** **4. Fixed problem of system hanging when installing Linux OS after COM1 & COM2 IO/IRQ exchange.** **5. Fixed problem of SUM GetSataInfo showing incorrect "Configuration Type" when setting "Configure sSATA as" to "AHCI" or "RAID" on sSATA controller.** **6. Fixed issue with IPMI firmware to enable storage card to show temperature.**

Release Notes from Previous Release(s)

2.0b (2/24/2018)

1. Updated CPU microcode to address CVE-2017-5715 security patch issue.
2. Updated Purley RC 151.R03.
3. Changed RC default setting to upgrade POST Memory correctable error to uncorrectable error and map out the channel.
4. Patched for inability of AOC-MH25G-b2S2G to show sensor.
5. Disabled CPU2 IIO PCIe root port ACPI hot plug function.
6. Fixed inability of AOC-MTG-i4T to show sensor.
7. Fixed problem of SMC skipping first boot option in UEFI mode when retrying boot.
8. Fixed inability to reset the system under DOS by pressing "Ctrl-Alt-Del" on USB keyboard when "Port 60/64 Emulation" is disabled.
9. Fixed inability of some CPUs to display correct microcode revision under BIOS setup menu.

2.0 (11/30/2017)

1. Changed BIOS revision to 2.0.
2. Updated Purley RC 149.R09, SPS 4.0.04.294, ACM files, and CPU microcode.
3. Set message "BIOS cannot support downgrade to previous version or ROMID mismatch" to show when trying to downgrade BIOS or flash other model of BIOS.
4. Fixed problem of serial console output showing SMC logo when EarlyVideo logo item is disabled.
5. Fixed problem of the Last UCE report (mapout) DIMM sometimes not matching real UCE DIMM location.
6. Fixed problem of IPMI SEL logging "Memory training failure." and "No memory DIMM detected, install memory DIMMs." twice per reboot.
7. Fixed problem of TPM 1.2 PS index not being Write-Protected so that the content of TPM 1.2 PS index still can be modified after TPM 1.2 is nvLocked.
8. Fixed problem of changes to CPU core Enable/Disable in setup menu sometimes not taking effect on Windows OS.
9. Fixed problem of system hanging during BIOS flashing if Watch Dog function is enabled.
10. Fixed system reboots endlessly when equipping dTPM module.
11. Fixed inability of DMI Customized Information to preserve after user implements BIOSLoadDefault or CMOS Clear Action.