IPMI Firmware / BIOS Release Notes Form

Product Name	**X11DSF-E**
Release Version	**3.0a**
Release Date	**2/16/2019**
Previous Version	**2.1**
Update Category	**Recommended**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Added support for Purley Refresh platform.** **2. Updated AMI label 5.14_PurleyCrb_0ACLA038_BETA (BKC WW50).** **3. Added support for Monitor Mwait feature.** **4. Patched missing PSU information if backplane MCU reports wrong PSU information.** **5. Disabled "tRWSR Relaxation" by default.** **6. Set PCIe correctable and uncorrectable (non-fatal) error report to disabled by default.** **7. Added support for RFC4122 UUID format feature to set RFC4122 encoding from build time produced by IPMICFG 1.29 tool or newer.** **8. Disabled PCH "PCI-E Global ASPM Support".** **9. Set NVDIMM ADR timeout to 600us according to Intel PDG.**
New features	**N/A**

Fixes	**1. Fixed malfunction of disabling Watch Dog while flashing BIOS under OS.** **2. Fixed problem of BIOS always retrying boot when Re-Try Boot is Disabled.** **3. Fixed malfunction of support for LEGACY to EFI.** **4. Fixed failure of always turbo in new Linux kernel 7.2.** **5. Added workaround for failure of BIOS flash with 156 bytes PubKey (Error: "Secure Flash Rom Verify Fail").** **6. Fixed failure of CPU PBF (Prioritized Base Frequency).** **7. Fixed issue with the backplane NF1 NVMe hot plug-in.**

Release Notes from Previous Release(s)

2.1 (8/24/2018)

1. Updated CPU microcode to address 'Spectre' derivatives (CVE-2018-3639 & CVE-2018-3640) security issue.
2. Enabled BIOS secure flash upgrade feature (firmware signature).
3. Corrected BIOS/ME downgrade check for SPS 4.0.4.340 and later.
4. Displayed Memory DIMM PPR setup item.
5. Checked PCH SKU for QAT enabled board.
6. Added message "Secure Flash Recovery Image Verification Failed." for prompting user if secure flash recovery image is invalid.
7. Updated SPS 4.0.4.381 for INTEL-SA-00131 Security Advisory to address CVE-2018-3643 and CVE-2018-3644 security issues.
8. Fixed failure of WDT function.
9. Fixed inability of system to clean event log via Afu command "/CLNEVNLOG".
10. Fixed issue with IPMI firmware to enable storage card to show temperature.