IPMI Firmware / BIOS Release Notes Form

Product Name	**X11DPL-i**
Release Version	**3.2**
Release Date	**12/2/2019**
Previous Version	**3.1**
Update Category	**Critical**
Dependencies	**N/A**
Important Notes	**ECO #23135** **BIOS Image X11DPLI9.C02** **Please update BIOS with attached Flash Utility in package.**
Enhancements	**1. Changed BIOS version to 3.2.** **2. Updated AMI label 5.14_PurleyCrb_0ACLA049_BETA for BKC WW36 IPU 2019.2 and AMI security update SA50072.** **3. Updated SINIT/BIOS ACM from BKC WW36 IPU 2019.2 address CVE-2019-0151 and CVE-2019-0152.** **4. Updated SPS_E5_04.01.04.339.0 from BKC WW36 IPU 2019.2 to address PSIRT-TA-201905-011.** **5. Updated Cascade Lake-SP CPU microcode and Skylake-SP microcode.** **6. Updated Cascade Lake-SP A0 stepping CPU microcode.** **7. Updated SATA/sSATA RAID OPROM/EFI driver to VROC PreOS v6.2.0.1034 PC.** **8. Displayed Setup item "ARI Support".** **9. Added setup item to control 16Gb based Single Die Package DIMM tRFC optimization.** **10. Updated Secure Boot Key to fix the error message of PK key.** **11. Added back erase NVDIMM routine.** **12. Updated VBIOS and VGA EFI Driver to 1.10.** **13. Enhanced F12 hot key PXE boot feature.** **14. Updated the behavior for the feature that updates SMBIOS Type 1**

	and 3 with FRU0. **15. Added Redfish/SUM Secure Boot feature to update OOB for secure boot and reserve Key.** **16. Disabled ADDDC/SDDC and set PPR as hPPR.** **17. Added sighting CLX28 workaround and downgraded patrol scrub UC to CE.**
New features	**1. Added Enhanced PPR function and set disabled as default.**
Fixes	**1. Removed PXE option for "OnBoard LanX Option ROM" when "Boot mode select" is UEFI.** **2. Corrected display of the IPMI AUX revision.** **3. Changed OOB download and Upload Bios Configuration sequence.** **4. Fixed problem of two OS (Redhat & Ubuntu) boot devices appearing in boot order.** **5. Fixed failure of OPROM control item if CSM is disabled.** **6. Fixed problem of key details showing "Security Violation" after loading Factory secure boot keys.**

Release Notes from Previous Release(s)

3.1 (5/21/2019)

1. *Updated Skylake-SP/Cascade Lake-SP CPU microcode.*
2. *Updated Intel BKCWW16 2019 PV PLR1.*
3. *Updated SPS_E5_04.01.04.296.0 from BKC WW16 2019.*
4. *Updated EIP467272 for AMI SA50069, SA50070.*
5. *Set SDDC Plus One or SDDC as Disabled by default.*
6. *Updated SATA/sSATA RAID OPROM/EFI driver to VROC PreOS v6.1.0.1017.*
7. *Set Leakey bucket to decrease one memory correctable error count within 2.15 minutes and threshold 512.*
8. *Set ADDDC Sparing to enable by default.*
9. *Fixed problem of system halting or rebooting at POST code 0xB2 or 0x92 when total GPT partition number is more than 256 and RSD is enabled.*

3.0b (3/4/2019)

1. *Added support for Purley Refresh platform.*
2. *Updated SPS to 4.1.04.256 (4.1.02.174 or above) for INTEL-SA-00185 Security Advisory RC to 576.D20 (549.D13 or above) for INTEL-SA-00192 Security Advisory.*
3. *Updated CPU microcode for Skylake-SP H0/M0/U0 stepping CPUs.*
4. *Added support for Monitor Mwait feature.*
5. *Set BMC MAC Address to UUID for system without onboard LAN1 or with onboard LAN1 disabled.*
6. *Updated SATA RAID OPROM/EFI driver to RSTe PreOS v6.0.0.1024.*
7. *Set PCIe correctable and uncorrectable (non-fatal) error report to disabled by default.*
8. *Added support for RFC4122 UUID format feature to set RFC4122 encoding from build time produced by IPMICFG 1.29 tool or newer.*
9. *Updated CPU microcode SRV_P_262 for Skylake-SP H0/M0/U0 CPUs.*
10. *Disabled unused SPS ME "CUPS IIO" and "Volumetric Airflow" sensor.*
11. *Added 2933 to memory POR.*
12. *Added support for Linux built-in utility efibootmgr.*
13. *Updated valid range of IPMI setup item VLAN ID to 1-4094.*
14. *Added driver health warning message.*
15. *Set NVDIMM ADR timeout to 600us..*
16. *Fixed malfunction of CPU PBF (Prioritized Base Frequency).*
17. *Fixed problem of setup item "Quiet Boot" staying enabled after flashing BIOS with "Quiet Boot" disabled.*
18. *Fixed incorrect PBF high frequency core number when Hyper-Threading is disabled.*
19. *Added workaround for failure of BIOS flash with 156 bytes PubKey (Error: "Secure Flash Rom Verify Fail").*
20. *Modified UEFI network description to IPv4/IPv6 to follow Industry Standard.*
21. *Patched problem of system hanging at 0x94 when plugging in Nvidia Tesla T4 card.*

2.1 (6/15/2018)

1. *Updated CPU microcode to address 'Spectre' derivatives (CVE-2018-3639 & CVE-2018-3640) security issue.*
2. *Changed BIOS version to 2.1.*
3. *Updated Purley RC 154.R13, SPS 4.0.04.340 and ACM 1.3.7, SINIT ACM 1.3.4.*
4. *Updated SATA RAID OPROM/EFI driver to RSTe PreOS v5.4.0.1039.*
5. *Added BIOS/ME downgrade check for SPS 4.0.4.340.*

6. *Added support for UEFI mode PXE boot of F12 hot key Net boot.*
7. *Added one event log to record that the event log is full.*
8. *Displayed PPR setup item.*
9. *Added support for SATA FLR.*
10. *Fixed problem of SUM GetSataInfo showing incorrect "Configuration Type" when setting "Configure sSATA as" to "AHCI" or "RAID" on sSATA controller.*
11. *Fixed problem of Ctrl + Alt + Del causing system to hang after flashing BIOS.*
12. *Fixed problem of system hanging when installing Linux OS after COM1 & COM2 IO/IRQ exchange.*
13. *Rolled back SVN_3413 to fix failure of WDT function*.

2.0b (3/6/2018)

1. *Updated CPU microcode SRV_B_216 for Skylake-SP H0/M0/U0 stepping CPUs to address 'Spectre' variant 2 (CVE 2017-5715) security issue.*
2. *Changed BIOS version to 2.0b.*
3. *Updated 5.12_PurleyCrb_0ACFD085Beta for Purley Skylake platform PLR 4, BKC WW02.*
4. *Displayed setup item "ACS Control" to Enable/Disable PCIe Access Control Services Extended Capability, with Enabled as default.*
5. *Updated BIOS ACM 1.3.5 and SINIT ACM 1.3.3.*
6. *Disabled CPU2 IIO PCIe root port ACPI hot plug function.*
7. *Fixed IPMI force boot issue.*
8. *Fixed malfunction of "SMBIOS Preservation" Disabled.*
9. *Fixed problem of SMC skipping first boot option in UEFI mode when retrying boot.*
10. *Fixed inability to reset the system under DOS by pressing "Ctrl-Alt-Del" on USB keyboard when "Port 60/64 Emulation" is disabled.*
11. *Fixed inability of some CPUs to display correct microcode revision under BIOS setup menu.*
12. *Hid unused items "Onboard NVME1\2 Option ROM" in BIOS setup menu.*
13. *Fixed inability of IPMI Web to report correct information for customer PSU "GW-ERP1U450-2H".*

2.0 (11/29/2017)

1. *Changed BIOS revision to 2.0.*
2. *Updated SATA RAID OPROM/EFI driver to RSTe PreOS v5.3.0.1052.*
3. *Updated BIOS ACM 1.3.4.*
4. *Updated SPS to 4.0.4.294.*
5. *Updated CPU microcode SRV_P_214 for Skylake-EP H0/M0/U0 stepping CPUs.*
6. *Updated 5.12_PurleyCrb_0ACFD084_BETA for Purley Skylake platform PLR 3.1*
7. *Fixed problem of SNC being disabled once NVDIMM is present in system.*
8. *Fixed problem of DMI being cleared when SUM LoadDefaultBiosCfg is run.*