IPMI Firmware / BIOS Release Notes Form

Product Name	**X11DPU**
Release Version	**3.3a**
Release Date	**07/21/2020**
Build Date	**07/21/2020**
Previous Version	**3.3**
Update Category	**Critical**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1.[Enhancements][SmcHttpBoot] Delete repeated boot options which have description the same as the new description.** **2.[Enhancements] Add inband flash status event log to IPMI MEL.** **3.[Enhancements] Correct "Station MAC Address" display order when "Configuration Address Source" set to "Static".** **4.[Enhancements] Update Skylake-SP microcode 6906, Cascade Lake-SP microcode 2F01 for IPU2020.1** **5.[Enhancements] Update SATA/sSATA RAID OPROM/EFI driver to VROC PreOS v6.3.0.1005 PV.** **6. [Enhancements] Update AEP FW to 1.2.0.5435**
New features	**None**

Fixes	**1.[Fixes] Fix 6240R and some refresh 4 serial CPU freq. can't reach the highest when enabling mwait.** **2.[Fixes] Fixed Secure Erase - Password doesn't success and BIOS return "EFI_Device_Error" with SED: Seagate ST1000NX0353.** **3.[Fixes]firmware revision may not correct in BIOS Setup.** **4.[Fixes] Fixed System hang 0xB2 problem with some NVME device.**

Release Notes from Previous Release(s)

3.3(02/21/2020)

1. Patched problem of system hanging at 94 with new NVidia RTX 6000/8000.
2. Enabled saving memory CE location into PPR variable at runtime even if memory correctable error reporting is disabled.
3. Added sighting CLX28 workaround and downgraded patrol scrub UC to CE.
4. Added SMC HDD Security feature.
5. Updated AMI label 5.14_PurleyCrb_0ACLA050 beta for IPU2020.1 PV.
6. Updated SPS_E5_04.01.04.381 from IPU 2020.1 PV.
7. Updated BIOS ACM 1.7.40 and SINIT ACM 1.7.48 PW.
8. Added setup item "HDD word prompt Control" to control "Hard-Drive word Check" for enabling/disabling HDD word prompt window during POST.
9. Updated Skylake-SP/Cascade Lake-SP CPU microcode for Intel-SA-00329 (CVE2020-0548 2.8 Low and CVE2020-0549 6.5 Medium), Intel-SA-00288 (CVE2019-11157 5.3 Medium), and Intel-SA-00317 (CVE2019-14607 7.9 High).
10. Fixed mismatch of Secure Boot Mode value.
11. Removed requirement to use Admin password for erasing TCG device.
12. Fixed problem of two CentOS boot items occurring in boot order if CentOS is installed in RAID 1 system.

3.2 (10/16/2019)

1. Updated AMI label 5.14_PurleyCrb_0ACLA049_BETA for BKC WW36 IPU 2019.2 and AMI security update SA50072.
2. Updated SINIT/BIOS ACM from BKC WW36 IPU 2019.2 to address CVE-2019-0151 and CVE-2019-0152.
3. Updated SPS_E5_04.01.04.339.0 from BKC WW36 IPU 2019.2 to address PSIRT-TA-201905-011.
4. Updated Cascade Lake-SP CPU microcode and Skylake-SP microcode.
5. Displayed Setup item "ARI Support".
6. Added setup item to control 16Gb based Single Die Package DIMM tRFC optimization.
7. Disabled ADDDC/SDDC and set PPR as hPPR.
8. Added Enhanced PPR function and set disabled as default.
9. Removed PXE option for "OnBoard LanX Option ROM" when "Boot mode select" is UEFI.
10. Corrected display of the IPMI AUX revision.

3.1a (07/19/2019)

1. Updated Skylake-SP/Cascade Lake-SP CPU microcode.
2. Updated SPS_E5_04.01.04.323 from BKC WW26 2019.
3. Updated Intel BKCWW26 2019 PV PLR2.
4. Enhanced F12 hot key PXE boot feature.
5. Updated Secure Boot Key to fix the error message of PK key.
6. Updated the behavior for the feature that updates SMBIOS Type 1 and 3 with FRU0.
7. Patched inability of system to boot via onboard LAN2 after IPMI forces PXE boot when there is an OS behind LSI-3108 RAID card.
8. Added back erase NVDIMM routine.
9. Removed Intel Virtualization Technology override when set to extreme performance.
10. Fixed problem of two OS (Redhat & Ubuntu) boot devices appearing in boot order.
11. Fixed failure of OPROM control item if CSM is disabled.

3.1 (04/29/2019)

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 to disabled by default.
6. Updated SATA/sSATA RAID OPROM/EFI driver to VROC PreOS v6.1.0.1017.
7. Set Leaky Bucket that can decrease one memory correctable error count within 2.15 minutes with threshold 512.
8. 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.
9. Fixed inability to change IPv6 address or IPv6 Router1 IP address.

3.0c (03/27/2019)

1. Added support for Purley Refresh platform.
2. Enhanced BIOS setup menu to auto-switch the Option ROM's value and hide the unexpected value when boot mode changes.
3. Updated to SPS 4.0.04.381 or above for INTEL-SA-00213 Security Advisory.
4. Fixed problem of UUID showing IPMI MAC incorrectly after disabling onboard LAN chip.
5. Temporarily fixed error for SKX (CLX) 4114 CPU memory training with Micron (18ASF2G72PDZ-2G6E1) RDIMM.
6. Fixed failure to boot into VMware OS when set to Maximum Performance even if Monitor/MWAIT is enabled.

3.0b (03/04/2019)

1. Added support for Purley Refresh platform.
2. Added support for Linux built-in utility efibootmgr.
3. Updated valid range of IPMI setup item VLAN ID to 1-4094.
4. Set NVDIMM ADR timeout to 600us.
5. Added driver health warning message.
6. Updated to SPS 4.1.02.174 or above for INTEL-SA-00185 Security Advisory and RC 549.D13 or above for INTEL-SA-00192 Security Advisory.
7. Modified UEFI network description to IPv4/IPv6 to follow Industry Standard.
8. Patched problem of system hanging at 0x94 when plugging in Nvidia Tesla T4 card.

3.0a (12/21/2018)

1. Added support for Purley Refresh platform.
2. Updated SATA RAID OPROM/EFI driver to RSTe PreOS v6.0.0.1024.
3. Set BMC MAC address to UUID for system without onboard LAN1 or with onboard LAN1 disabled.
4. Set PCIe correctable and uncorrectable (non-fatal) error report to disabled by default.
5. Set RFC4122 encoding to only be enabled for build time produced by IPMI 1.29 or newer.
6. Updated CPU microcode SRV_P_262 for Skylake-SP H0/M0/U0 CPUs.
7. Disabled unused SPS ME "CUPS IIO" and "Volumetric Airflow" sensor.
8. Added 2933 to memory POR.
9. Added support for SATA FLR.
10. Added support for Monitor Mwait feature.
11. Disabled "tRWSR Relaxation" by default.
12. Fixed problem of setup item "Quiet Boot" staying enabled after flashing BIOS with "Quiet Boot" disabled.
13. Added workaround for GPU P2P low bandwidth.
14. Fixed malfunction of disabling Watch Dog while flashing BIOS under OS.
15. Corrected standard NVDIMM ADR time.
16. Fixed failure of CPU PBF (Prioritized Base Frequency).

2.1b (10/16/2018)

1. Added SATA FLR support.
2. Added support for Monitor Mwait feature.
3. Updated SPS 4.0.4.393.
4. Updated CPU microcode SRV_P_253 for Skylake-SP H0/M0/U0 stepping CPUs.
5. Updated SATA RAID OPROM/EFI driver to RSTe PreOS v5.5.0.1028.
6. Updated BIOS ACM 1.3.9 and SINIT ACM 1.3.6.
7. Changed Onboard LAN SMBIOS table from type 9 to type 41.
8. Fixed problem of BIOS always retrying boot when Re-Try Boot is Disabled.
9. Fixed malfunction of LEGACY to EFI support.

_____ _____

Product Manager *Date*