BIOS Release Notes Form

Product Name	**X11SPG-TF**
Release Version	**4.0**
Release Date	**6/20/2023**
Build Date	**6/20/2023**
Previous Version	**3.9**
Update Category	**Recommended**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Changed BIOS revision to 4.0.** **2. Updated AMI label 5.14_PurleyCrb_0ACLA060 for RC0628.P50 IPU 2023.3.** **• For INTEL-SA-00813 Security Advisory to address CVE-2022-37343(7.2, High), CVE-2022-44611(6.9, Medium), CVE-2022-38083(6.1, Medium), CVE-2022-27879(5.3, Medium) and CVE-2022-43505(4.1, Medium) security issues.** **• For INTEL-SA-00828 Security Advisory to address CVE-2022-40982(6.5, Medium) security issue.** **3. Updated token RC_VERSION_VALUE setting to 628.P50. Updated token PRICESSO_0_UCODE_VERSION setting to 02007006. Updated token PRICESSO_2_UCODE_VERSION setting to 04003604. Updated token**

	PRICESSO_3_UCODE_VERSION setting to 05003604. Update token FW_SPS_VERSION setting to 4.1.5.2. **4. Updated Cascade Lake-SP CPU PV microcode for IPU 2023.3.** **5. Updated Intel Server Platform Services for Purley Refresh Server Platforms IPU2023.3 4.1.5.2.** **6. Updated DBX file for AMI-SA50182 Secure Boot DBX Update.**
New features	**N/A**
Fixes	**N/A**

Release Notes from Previous Release(s)

3.9 (3/15/2023)

1. *Changed BIOS revision to 3.9.*
2. *Updated AMI label 5.14_PurleyCrb_0ACLA059 for RC0627.P11 IPU 2023.2 for INTEL-SA-00807 Security Advisory to address CVE-2022-38087(4.1, Medium) and CVE-2022-33894(7.5, High) security issues; and for INTEL-SA-00717 Security Advisory to address CVE-2022-32231 (7.5, High) / CVE-2022-26343 (8.2, High) security issues.*
3. *Updated token RC_VERSION_VALUE setting to 627.P11. Updated token PRICESSO_0_UCODE_VERSION setting to 02006F05. Updated token PRICESSO_1_UCODE_VERSION setting to 03000012. Updated token PRICESSO_2_UCODE_VERSION setting to 04003501. Updated token PRICESSO_3_UCODE_VERSION setting to 05003501.*
4. *Updated Cascade Lake-SP CPU PV microcode for IPU 2023.2.*

3.8a (10/28/2022)

1. *Updated the AMI label 5.14_PurleyCrb_0ACLA057 for RC0623.D09 2022.3 IPU.*
2. *Updated token RC_VERSION_VALUE setting to 623.D09, token PRICESSO_0_UCODE_VERSION setting to 02006E05, and token FW_SPS_VERSION setting to 4.1.4.804.*
3. *Updated the Intel DCPM UEFI driver to 1.0.0.3536.*
4. *Updated Skylake-SP/Cascade Lake-SP CPU PC microcode for IPU 2022.2.*
5. *Fixed the wrong DIMM location display in the event log page.*
6. *Modified the string name SMCI to Supermicro.*
7. *Removed "Vendor Keys" in the security page.*
8. *Refined the SMM buffer validation in SmmSmbiosELogInitFuncs.c. Allocated the runtime buffer to trigger ELog SMI in DxeSmmRedirFuncs.c.*
9. *Updated BIOS ACM 1.7.54, SINIT ACM 1.7.55 PW for IPU2022.1 to address Intel-TA-00161: CVE-2021-0159 (7.8 High) CVE-2021-33123 (8.2 High) and CVE-2021-33124 (7.5 High).*
10. *Updated the VROC SATA/sSATA legacy driver to VROC PreOS v6.3.5.1003 Hot Fix to fix 10TB or higher volume drive issue.*
11. *Updated the VROC SATA/sSATA EFI driver to VROC PreOS v7.8.0.1012 to address: 1) Data Loss Exposure Due to RAID 5 TRIM Support. Document #737276. 2) INTEL-TA-00692. CVE-2022-29919(7.8 High), CVE-2022-30338(6.7 Medium), CVE-2022-29508(6.3 Medium), CVE-2022-25976(5.5 Medium).*
12. *Modified the allocated buffer from EfiBootServicesData to EfiRuntimeServicesData.*
13. *Disabled the MROM1 device since it doesn't use the Intel IE function.*
14. *Updated the DBX file to fix the Secure Boot Bypass issue.*
15. *Fixed the OA2 key injection issue.*
16. *Enabled IScsi_SUPPORT on the Purley generation.*

3.6 (1/3/2022)

1. *Changed BIOS revision to 3.6.*
2. *Updated SATA/sSATA EFI driver to VROC PreOS v7.7.0.1054.*
3. *Updated AEP uEFI driver to 1.0.0.3531 for IPU2021.2.*
4. *Updated AMI label 5.14_PurleyCrb_0ACLA054 for RC0616.D08 2021.2 IPU for INTEL-SA-00527 Security Advisory to address CVE-021-0103 (8.2, High), CVE-2021-0114 (7.9, High), CVE-2021-0115 (7.9, High), CVE-2021-0116 (7.9, High), CVE-2021-0117 (7.9, High), CVE-2021-0118 (7.9, High),*

CVE-2021-0099 (7.8, High), CVE-2021-0156 (7.5, High), CVE-2021-0111 (7.2, High), CVE-2021-0107 (7.2, High), CVE-2021-0125 (6.7, Medium), CVE-2021-0124 (6.3, Medium), CVE-2021-119 (5.8, Medium), CVE-2021-0092 (4.7, Medium), CVE-2021-0091 (3.2, Low) and CVE-2021-0093 (2.4, Low) security issues.

5. *Updated Intel Server Platform Services for Purley Refresh Server Platforms IPU2021.2 HF1 4.1.4.654.*
6. *Updated BIOS ACM 1.7.51, SINIT ACM 1.7.51 PW for INTEL-SA-00527 Security Advisory to address CVE-2021-0103 (8.2, High), CVE-2021-0114 (7.9, High), CVE-2021-0115 (7.9, High), CVE-2021-0116 (7.9, High), CVE-2021-0117 (7.9, High), CVE-2021-0118 (7.9, High), CVE-2021-0099 (7.8, High), CVE-2021-0156 (7.5, High), CVE-2021-0111 (7.2, High), CVE-2021-0107 (7.2, High), CVE-2021-0125 (6.7, Medium), CVE-2021-0124 (6.3, Medium), CVE-2021-0119 (5.8, Medium), CVE-2021-0092 (4.7, Medium), CVE-2021-0091 (3.2, Low) and CVE-2021-0093 (2.4, Low) security issues.*
7. *Updated Skylake-SP/Cascade Lake-SP CPU PV microcode for INTEL-SA-00532 Security Advisory to address CVE-2021-0127 (5.6, Medium) security issue and for INTEL-SA-00365 Security Advisory to address CVE-2020-8673 (4.7, Medium) security issue.*

3.5 (5/24/2021)

1. *Updated RC 612.D02 for INTEL-SA-00463 Security Advisory to address CVE-2020-12357(7.5, High), CVE-2020-8670(7.5, High), CVE-2020-8700(7.5, High), CVE-2020-12359(7.1, High), CVE-2020-12358(6.7, Medium), CVE-2020-12360(5.6, Medium), CVE-2020-24486(5.5, Medium) and CVE-2020-0589(3.8, Low) security issues.*
2. *Updated BIOS ACM 1.7.43, SINIT ACM 1.7.4A PW for INTEL-SA-00463 Security Advisory to address CVE-2020-12357(7.5, High), CVE-2020-8670(7.5, High), CVE-2020-8700(7.5, High), CVE-2020-12359(7.1, High), CVE-2020-12358(6.7, Medium), CVE-2020-12360(5.6, Medium), CVE-2020-24486(5.5, Medium) and CVE-2020-0589(3.8, Low) security issues.*
3. *Updated Skylake-SP/Cascade Lake-SP CPU PV microcode for INTEL-SA-00464 Security Advisory to address CVE-2020-24511(5.6, Medium) and CVE-2020-24512(2.8, Low) security issues.*
4. *Updated Intel Server Platform Services for Purley Refresh Server Platforms 4.1.4.505.*
5. *Enabled the BMC PXE boot command to detect LAN ports.*
6. *Updated the SATA/sSATA EFI driver to VROC PreOS v7.5.0.1152.*
7. *Enabled the system to boot into PXE with DVD installed.*
8. *Updated Intel Server Platform Services for Purley Refresh Server Platforms HF 4 PLR 4.1.4.450.*
9. *Added support for IPv6 HTTP boot.*
10. *Changed the spelling of the word "spectrum" the "PCIe PLL SSC" BIOS setting description.*
11. *Removed the 4G limit on the LAN memory for EFI boot mode.*
12. *Updated AEP FW to FW_1.2.0.5446, uEFI driver to 3515 for IPU2021.1.*
13. *Synched the IPv6 status in the BIOS settings and the BMC web page.*
14. *Fixed the IPv6 BIOS setting "Configuration Address Source" to show "Static" and allowed setting the IP address.*
15. *Fixed the names of the UEFI OS boot drives to show the full drive part numbers.*

3.4 (12/14/2020)

1. *Updated AMI label 5.14_PurleyCrb_0ACLA052_BETA for RC update and IPU 2020.2 PV to address Intel-TA-00358: CVE-2020-0587 (6.7, Medium), CVE-2020-0591 (6.7, Medium), and CVE-2020-0592 (3, Low); Intel-TA-00390: CVE-2020-0593 (4.7, Medium), CVE-2020-8738 (7.5, High), CVE-2020-8739 (4.6, Medium), CVE-2020-8740 (6.7, Medium), and CVE-2020-8764 (8.7, High); Intel-TA-00391: CVE-2020-8752 (9.4, Critical), CVE-2020-8753 (8.2, Critical), CVE-2020-12297 (8.2, Critical), CVE-2020-8745 (7.3, Critical), CVE-2020-8705 (7.1, Critical), CVE-2020-12303 (7.0, Critical), CVE-*

2020-8757 (6.3, Medium), CVE-2020-8756 (6.3, Medium), CVE-2020-8760 (6.0, Medium), CVE-2020-8754 (5.3, Medium), CVE-2020-8747 (4.8, Medium), CVE-2020-12356 (4.4, Medium), CVE-2020-8746 (4.3, Medium), and CVE-2020-8749 (4.2, Medium); Intel-SA-00358: CVE-2020-0590 (7.7, High), CVE-2020-0587 (6.7, Medium), CVE-2020-0591 (6.7, Medium), CVE-2020-0593 (4.7, Medium), CVE-2020-0588 (3.8, Low), and CVE-2020-0592 (3.0, Low); Intel-TA-00391: CVE-2020-8744 (7.2, High), CVE-2020-8705 (7.1, High), and CVE-2020-8755 (4.6, Medium); AMI SA50080 and AMI SA50081: CVE-2020-0570 (7.6, High), CVE-2020-0571 (5.5, Medium), and CVE-2020-8675 (7.1, High); AMI SA-50085: CVE-2020-10713 (8.2, High); and AMI SA-50084: CVE-2020-10255 (9, High) security issues.

2. *Added force next boot to UEFI Shell via IPMI support.*
3. *Added function to move all LANs to the top of boot priority when IPMI forces PXE.*
4. *Updated SATA/sSATA RAID OPROM/EFI driver to VROC PreOS v6.3.0.1005 PV.*
5. *Updated AEP firmware to FW_1.2.0.5444 to match IPU2020.2.*
6. *Deleted repeated boot options which have the same description as the new description.*
7. *Added inband flash status event log to IPMI MEL.*
8. *Corrected "Station MAC Address" display order when "Configuration Address Source" is set to "Static."*
9. *Fixed problem of EFI version of PassMark MemTest86 hanging when SMCI Redfish Host Interface is not supported in IPMI firmware.*
10. *Fixed failure of Secure Erase - Password and problem of BIOS returning "EFI_Device_Error" with SED: Seagate ST1000NX0353.*
11. *Corrected BMC firmware revision in BIOS Setup.*
12. *Fixed problem of system hanging at 0xB2 with some NVMe devices.*
13. *Enabled ONBOARD_LAN_DROP_CHECK to correct for issue of onboard LAN gen dropping.*

3.3 (2/21/2020)

1. *Updated AMI label 5.14_PurleyCrb_0ACLA050 beta for IPU2020.1 PV.*
2. *Updated BIOS ACM 1.7.40 and SINIT ACM 1.7.48 PW.*
3. *Added support for SMCI USB Remote Network Driver Interface and SMCI USB Universal Network Device Interface, and for Redfish module to get Processor, Memory, and PCIe information.*
4. *Enabled saving memory CE location into PPR variable at runtime even if memory correctable error reporting is disabled.*
5. *Added setup item "HDD password prompt" to enable/disable HDD password prompt window during POST.*
6. *Added sighting CLX28 workaround and downgraded patrol scrub UC to CE.*
7. *Updated Skylake-SP/Cascade Lake-SP CPU microcode from Intel-Restricted-2020-1-IPU limit beta.*
8. *Added SMC HDD Security feature.*
9. *Added support for SUM Feature flags 1.8.*
10. *Updated setup menu to remove our own tRFC optimization item, add Intel "tRFC Optimization for 16Gb Based DIMM" and "Panic and High Watermark" items, and add "Balanced Profile" option for "DCPMM Performance Setting".*
11. *Updated SPS_E5_04.01.04.381 from IPU 2020.1 PV.*
12. *Fixed issue of system resetting under ATTO Fiber network card user menu during BIOS POST.*
13. *Forced ATTO fibre channel to 32bit address and Intel 100G NIC (AOC-S100GC-i2C) to 64bit address.*
14. *Fixed mismatch of Secure Boot Mode value.*
15. *Fixed malfunction of onboard SAS option ROM control.*
16. *Fixed Intel Self-test 7 v111 SPI/DCh BIOS_CNTL to set BIOS Control Register BIT[9] to 1.*
17. *Fixed inability to log UPI correctable error.*
18. *Fixed problem of system hanging at POST code 0x92 with Apacer M.2 SSD.*

19. *Removed requirement to use Admin password for erasing TCG device.*
20. *Fixed problem of two CentOS boot items occurring in boot order if CentOS is installed in RAID 1 system.*

3.2 (11/27/2019)

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. *Updated Secure Boot Key to fix the error message of PK key.*
8. *Patched inability of system to boot via onboard LAN2 after IPMI forces PXE boot when there is an OS behind LSI-3108 RAID card.*
9. *Added back erase NVDIMM routine.*
10. *Updated VBIOS and VGA EFI Driver to 1.10.*
11. *Enhanced F12 hot key PXE boot feature.*
12. *Updated the behavior for the feature that updates SMBIOS Type 1 and 3 with FRU0.*
13. *Added support for SMC HttpBoot.*
14. *Disabled ADDDC/SDDC and set PPR as hPPR.*
15. *Patched problem of system hanging at 94 with new NVidia RTX 6000/8000.*
16. *Added sighting CLX28 workaround and downgraded patrol scrub UC to CE.*
17. *Added Enhanced PPR function and set disabled as default.*
18. *Removed PXE option for "OnBoard LanX Option ROM" when "Boot mode select" is UEFI.*
19. *Corrected display of the IPMI AUX revision.*
20. *Changed OOB download and Upload Bios Configuration sequence.*
21. *Fixed problem of two OS (Redhat & Ubuntu) boot devices appearing in boot order.*
22. *Fixed failure of OPROM control item if CSM is disabled.*

3.1 (5/27/2019)

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.*
10. *Set ADDDC to enabled by default.*
11. *Fixed problem of windows showing yellow marks under device manager after installing driver CD.*

3.0b (3/11/2019)

1. *Added support for Purley Refresh platform.*
2. *Updated SATA RAID OPROM/EFI driver to RSTe PreOS v6.0.0.1024.*
3. *Set PCIe correctable and uncorrectable (non-fatal) error report to disabled by default.*
4. *Added support for RFC4122 UUID format feature to set RFC4122 encoding from build time produced by IPMICFG 1.29 tool or newer.*
5. *Updated CPU microcode SRV_P_262 for Skylake-SP H0/M0/U0 stepping CPUs.*
6. *Disabled unused SPS ME "CUPS IIO" and "Volumetric Airflow" sensor.*
7. *Added 2933 to memory POR.*
8. *Added support for Linux built-in utility efibootmgr.*
9. *Updated valid range of IPMI setup item VLAN ID to 1-4094.*
10. *Added Driver Health warning message.*
11. *Set NVDIMM ADR timeout to 600us.*
12. *Prevented inability to flash BIOS by AFU or SUM inband when JPME2 CMOS value is not accepted.*
13. *Added a help/reminder message when a user incorrectly selects "EFI" for "Onboard Video Option Room" to avoid user confusion.*
14. *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.*
15. *Fixed problem of setup item "Quiet Boot" staying enabled after flashing BIOS with "Quiet Boot" disabled.*
16. *Fixed failure of workaround for BIOS flash with 156 bytes PubKey (Error: "Secure Flash Rom Verify Fail").*
17. *Modified UEFI network description to IPv4/IPv6 to follow Industry Standard.*
18. *Patched system from hanging 0x94 when plugging in NVIDIA Tesla T4 card.*
19. *Fixed incorrect display of TDP in Intel Speed Select table.*
20. *Fixed failure of AOC sensor reading when directly plugging a PCIe card in CPU PCI slot.*

2.1a (9/5/2018)

1. *Set PCIe link status to be polled at DXE stage to fix wrong information in BIOS setup IIO page.*
2. *Changed MAX_ITEM_STRING_SIZE to 128 bytes when updating Help string by SetString.*
3. *Updated SPS 4.0.4.381 for INTEL-SA-00131 Security Advisory to address CVE-2018-3643 and CVE-2018-3644 security issues.*
4. *Added support for Monitor Mwait feature.*
5. *Added support for IPV6 address multiline feature on IPMI page.*
6. *Updated 5.12_PurleyCrb_0ACFD089Beta security update.*
7. *Added a patch to prevent reboot hang when installing AVAL APX-3224 card.*
8. *Added support for SATA FLR.*
9. *Fixed failure of system downgrade from SPS 4.0.4.381 to 4.0.4.340.*
10. *Fixed failure of turbo in new Linux kernel.*
11. *Patched missing PSU information if common header is empty.*
12. *Fixed issue with IPMI firmware capability for SIOM projects.*
13. *Fixed malfunction of support for LEGACY to EFI.*
14. *Fixed problem of BIOS always retrying boot when Re-Try Boot is Disabled.*
15. *Fixed malfunction of BIOS/ME downgrade check when running flash package (SWJPME2) a second time.*
16. *Fixed problem of system resetting while flashing BIOS under OS if Watch Dog function is enabled.*
17. *Added workaround for low GPU P2P bandwidth.*

18. *Fixed problem of system always rebooting after flashing BIOS that has password preset and quiet boot disabled.*

2.1 (6/19/2018)

1. *Updated CPU microcode to address 'Spectre' derivatives (CVE-2018-3639 & CVE-2018-3640) security issue.*
2. *Corrected default setting for Enable SmcBusMasterEn setup item.*
3. *Added BIOS/ME downgrade check for SPS 4.0.4.340.*
4. *Added hidden item "Early Console Logo".*
5. *Added support for RFC3021.*
6. *Added support for UEFI mode PXE boot of F12 hot key Net boot.*
7. *Changed X11SPG BIOS revision to 2.1.*
8. *Updated Purley RC 154.R13, SPS 4.0.04.340 and ACM 1.3.7, SINIT ACM 1.3.4.*
9. *Updated SATA RAID OPROM/EFI driver to RSTe PreOS v5.4.0.1039.*
10. *Corrected BIOS/ME downgrade check for SPS 4.0.4.340.*
11. *Corrected help message for TPH BIOS setup items.*
12. *Displayed PPR setup item.*
13. *Fixed inability of AFUWIN to keep VMD setting.*
14. *Fixed problem of SUM GetSataInfo showing incorrect "Configuration Type" when setting "Configure sSATA as" to "AHCI" or "RAID" on sSATA controller.*
15. *Fixed problem of DMI being cleared when running SUM UpdateBios.*
16. *Updated 10G LAN EFI driver 6.7.0.4 (IBA 23.1) to address onboard X540 UEFI PXE failure issue.*
17. *Fixed problem of system hanging when installing Linux OS after COM1 & COM2 IO/IRQ exchange.*
18. *Fixed problem of Ctrl + Alt + Del causing system to hang after flashing BIOS.*

2.0b (2/26/2018)

1. *Updated CPU microcode to address 'Spectre' variant 2 (CVE 2017-5715) security issue.*
2. *Added setup item "SmcBusMasterEn" for enabling Parent bridge of the devices in the gSmcPciForceEnableBusMasterList.*
3. *Updated "Power Technology" callback solution.*
4. *Added support for VMD settings to be preserved after flashing, with disabled as default.*
5. *Updated 5.12_PurleyCrb_0ACFD085Beta for Purley Skylake platform PLR 4, BKC WW02.*
6. *Displayed setup item "ACS Control" to Enable/Disable PCIe Access Control Services Extended Capability, with Enabled as default.*
7. *Fine-tuned maximum payload for NVMe device.*
8. *Enabled IERR crash dump function.*
9. *Added MMIO prelocation for JBOF NVMe.*
10. *Changed maximum speed in SMBIOS type 4 to 4500Mhz.*
11. *Added one event log to record that the event log is full.*
12. *Added support for VMD settings to be preserved after flashing, with enabled as default.*
13. *Changed RC default setting to upgrade POST Memory correctable error to uncorrectable error and map out the channel.*
14. *Added UIO LAN control function.*
15. *Implemented SMC OOB TPM Provisioning via IPMI Feature for customized provisioning table.*
16. *Fixed inability of BIOS to boot into OS with Intel P3608 PCIe NVMe drive installed.*
17. *Fixed issue with IPMI force boot.*

18. *Fixed issue of all commands requesting to be persistent.*
19. *Fixed problem of incorrect memory access on OOB causing system to hang.*
20. *Fixed malfunction of "SMBIOS Preservation" Disabled.*
21. *Fixed problem of SMC skipping first boot option in UEFI mode when retrying boot.*
22. *Fixed problem of the endpoint PCIe device having error bits in PCI Status or Device Status register.*
23. *Fixed inability to set memory policy.*
24. *Fixed inability to reset the system under DOS by pressing "Ctrl-Alt-Del" on USB keyboard when "Port 60/64 Emulation" is disabled.*
25. *Fixed problem of some platforms hanging up at POST code 0xB2 when equipping dTPM module.*
26. *Fixed problem of DMI being cleared when running SUM LoadDefaultBiosCfg.*
27. *Fixed problem of TPM 2.0 PS NV Index not being write-protected even if customized provisioning table indicates that it must be write-protected when using "SMC OOB TPM Provisioning via IPMI feature".*
28. *Fixed problem of system hanging during BIOS flashing if Watch Dog function is enabled.*
29. *Corrected the "Save Changes" setup option string in "Save & Exit" menu.*
30. *Disabled SNC once NVDIMM is present in system.*
31. *Fixed problem of changing CPU Core Enable/Disable in setup menu sometimes not taking effect on Windows OS.*
32. *Fixed problem of system generating abnormal strings under DOS after triggering SERR or PERR error event in PCH slot.*
33. *Fixed inability of some CPUs to display correct microcode revision under BIOS setup menu.*