IPMI Firmware / BIOS Release Notes Form

Product Name	**X11DSC+**
Release Version	**3.8b**
Release Date	**1/6/2023**
Previous Version	**3.8a**
Update Category	**Recommended**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1.[Enhancements] Change BIOS revision to 3.8b.** **2.[Enhancements] Update AMI label 5.14_PurleyCrb_0ACLA058 for RC0626.P01 IPU 2023.1 (1). For INTEL-SA-00717 Security Advisory to address CVE-2022-32231 (7.5, High) / CVE-2022-26343 (8.2, High) security issues.** **3.[Enhancements] Update token RC_VERSION_VALUE setting to 626.P01.** **4.[Enhancements] Updated Cascade Lake-SP CPU PV microcode for IPU 2023.1.**
New features	**None**
Fixes	**None**

Release Notes from Previous Release(s)

3.8a(10/28/2022)

1.[Enhancements] Change BIOS revision to 3.8a.
2.[Enhancements] Update SATA/sSATA EFI driver to VROC PreOS v7.7.0.1054.
3.[Enhancements] Update AEP uEFI driver to 1.0.0.3531 for IPU2021.2.
4.[Enhancements] Update AMI label 5.14_PurleyCrb_0ACLA054 for RC0616.D08 2021.2 IPU. 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.
5.[Enhancements] Updated Intel Server Platform Services for Purley Refresh Server Platforms IPU2021.2 HF1 4.1.4.654.
6.[Enhancements] Update 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.[Enhancements] Updated Skylake-SP/Cascade Lake-SP CPU PV microcode. Updated Skylake-SP H0/M0/U0 stepping CPU
PV microcode MB750654_02006C0A. Update Cascade Lake-SP B0 stepping CPU PV microcode MBF50656_0400320A.
Update Cascade Lake-SP B1 stepping CPU PV microcode MBF50657_0500320A. For INTEL-SA-00532 Security Advisory to
address CVE-2021-0127(5.6, Medium) security issue. For INTEL-SA-00365 Security Advisory to address CVE-2020-8673(4.7,
Medium) security issue.
8.[Enhancements] Update AMI label 5.14_PurleyCrb_0ACLA056 for RC0622.D07 2022.2 IPU. (1). For INTEL-SA-00601 Security
Advisory to address CVE-2021-0154(8.2, High), CVE-2021-0153(8.2, High), CVE-2021-33123(8.2, High), CVE-2021-0190(8.2,
High), CVE-2021-33122(7.9, High), CVE-2021-33060(7.8, High), CVE-2021-0189(7.5, High), CVE-2021-33124(7.5, High), CVE-
2021-33103(7.5, High), CVE-2021-0159(7.4, High), CVE-2021-0188(5.3, Medium) and CVE-2021-0155(4.4, Medium) security
issues. (2). For INTEL-SA-00615 Security Advisory to address CVE-2022-21123(6.1, Medium), CVE-2022-21127(5.6, Medium),
CVE-2022-21125(5.5, Medium) and CVE-2022-21166(5.5, Medium) security issues. (3). For INTEL-SA-00616 Security Advisory
to address CVE-2021-21131(3.3, Low) and CVE-2021-21136(2.7, Low) security issues.

9.[Enhancements] Updated Skylake-SP/Cascade Lake-SP CPU PC microcode for IPU 2022.2. (1). For INTEL-SA-00601 Security
Page 1 of 4 SM Form #123, Rev. H (Issued 01/08/16)
Advisory to address CVE-2021-0154(8.2, High), CVE-2021-0153(8.2, High), CVE-2021-33123(8.2, High), CVE-2021-0190(8.2,
High), CVE-2021-33122(7.9, High), CVE-2021-33060(7.8, High), CVE-2021-0189(7.5, High), CVE-2021-33124(7.5, High), CVE-
2021-33103(7.5, High), CVE-2021-0159(7.4, High), CVE-2021-0188(5.3, Medium) and CVE-2021-0155(4.4, Medium) security
issues. (2). For INTEL-SA-00615 Security Advisory to address CVE-2022-21123(6.1, Medium), CVE-2022-21127(5.6, Medium),
CVE-2022-21125(5.5, Medium) and CVE-2022-21166(5.5, Medium) security issues. (3). For INTEL-SA-00616 Security Advisory
to address CVE-2021-21131(3.3, Low) and CVE-2021-21136(2.7, Low) security issues.
10.[Enhancements] Update token RC_VERSION_VALUE setting to 622.D07. Update token PRICESSO_0_UCODE_VERSION
setting to 02006E05. Update token FW_SPS_VERSION setting to 4.1.4.804.
11.[Enhancements] Fix show wrong DIMM location in event log page.
12.[Enhancements] Modify String naming from SMCI to Supermicro.
13.[Enhancements] Remove "Vendor Keys" in security page.
14.[Enhancements] [SMIHandlerSecurityFix] 1.Refine SMM buffer validation in SmmSmbiosELogInitFuncs.c 2.Allocate runtime
buffer to trigger ELog SMI in DxeSmmRedirFuncs.c
15.[Enhancements] Update AEP uEFI driver to 01.00.00.3534 for IPU2022.2.
16.[Enhancements] Update 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)
17.[Enhancements] Update 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)
18.[Enhancements] Modify the allocated buffer from EfiBootServicesData to EfiRuntimeServicesData.
19.[Enhancements] Disable MROM1 device since product doesn't use Intel IE function.
20.[Enhancements] Update DBX file to fix Secure Boot Bypass issue.
21.[Enhancements] Update AMI label 5.14_PurleyCrb_0ACLA057 for RC0623.D09 2022.3 IPU. (1) For INTEL-TA-00610 Security
Advisory to address CVE-2022-26845 (8.7 High), CVE-2022-27497(8.6 High), CVE-2022-29893 (8.1 High), CVE-2021-33159
(7.4 High), CVE-2022-29466(7.3 High), CVE-2022-29515(6.0 Medium) security issues. (2) For INTEL-TA-00688 Security Advisory
to address CVE-2022-26006 (8.2 High), CVE-2022-21198(7.9 High) security issues.
22.[Enhancements] Update token RC_VERSION_VALUE setting to 623.D09. Update token PRICESSO_0_UCODE_VERSION
setting to 02006E05. Update token FW_SPS_VERSION setting to 4.1.4.804.
23.[Enhancements] Update Intel DCPM UEFI driver to 1.0.0.3536.

3.5(06/01/2021)
1.[Enhancements] Update 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.[Enhancements] Update 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.[Enhancements] 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.[Enhancements] Updated Intel Server Platform Services for Purley Refresh Server Platforms 4.1.4.505.
5.[Enhancements] Support IPMI UEFI PXE boot to all LAN port feature.
6.[Enhancements] Update SATA/sSATA EFI driver to VROC PreOS v7.5.0.1152.
7.[Enhancements] This system cannot boot into PXE with DVD installed.
8.[Enhancements] Support IPv6 HTTP Boot function.
9.[Enhancements] Correct typo in "PCIe PLL SSC" setup item help string.
10.[Enhancements] Remove intel lan memory 4G limit if boot mode is not legacy.
11.[Enhancements] Update AEP FW to FW_1.2.0.5446, uEFI driver to 3515 for IPU2021.1.
12.[Enhancements] Sync IPv6 status detection rule with BMC to make sure IPv6 status is the same in BIOS and BMC web.
13.[Fixes] Fix "Configuration Address Source" always show "DHCP" in IPMI IPv6 page.
14.[Fixes] Fixed UEFI OS boot option name shows incorrectly in BIOS setup.

3.4 (02/05/2021)
1.[Enhancements] Updated BIOS ACM 1.7.41, SINIT ACM 1.7.49 PW to addresses Intel-TA-00358: CVE-2020-0588 (3.8 Low) and CVE-2020-0590. (7.7 High)
2.[Enhancements] Updated SPS 4.1.4.423 to address Intel-TA-00391: CVE-2020-8755 (4.6 Medium) CVE-2020-8705 (7.1 High)
3.[Enhancements] Updated Skylake-SP/Cascade Lake-SP CPU PV microcode from 20200918_NDA Release to address Intel-TA-00381: CVE-2020-8696 (2.5 Low) and MD_Clear Errata, MOB Speedpath and IRR Restore with RS Throttle (ITR #2).
4.[Enhancements] Enhanced SMCI HDD Security feature.
5.[Enhancements] Added force next boot to UEFI Shell via IPMI support.
6.[Enhancements] Added function to move all LANs to the top of boot priority when IPMI force PXE.
7.[Enhancements] Add inband flash status event log to IPMI MEL.
8.[Enhancements] Correct "Station MAC Address" display order when "Configuration Address Source" set to "Static".
9.[Enhancements] Support AOC-SHG3-4M2P card sensor reporting in VMD mode.
10.[Enhancements] Update 5.14_PurleyCrb_0ACLA052_BETA for RC update and 2020.2 IPU PV to addresses Intel-TA-00358: CVE-2020-0587 (6.7 Medium), CVE-2020-0591 (6.7 Medium), 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), 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), 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), CVE-2020-0592(3.0, Low). INTEL-TA-00391: CVE-2020-8744(7.2, High), CVE-2020-8705(7.1, High), 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) AMI SA-50084: CVE-2020-10255 (9, High)
11.[Enhancements] Updated Intel Server Platform Services for Purley Refresh Server Platforms HF 4 PLR 4.1.4.450
12.[Enhancements] Updated Skylake-SP/Cascade Lake-SP CPU PV microcode from 20210125_NDA Release
13.[Enhancements] Update SATA/sSATA EFI driver to VROC PreOS v7.5.0.1150.
14.[Enhancements] Support IPMI UEFI PXE boot to all LAN port feature.
15.[Enhancements] This system cannot boot into PXE with DVD installed.
16.[Fixes] Update AMI EIP563137 to fix some BIOS items (like boot mode item) load default failure issue with some configurations (like with Micron M.2 or HGST SATA M.2)
17.[Fixes] Fixed UEFI SCT test found the "UEFI Compliant - Boot from iSCSI peripheral" fail.
18.[Fixes] Fixed system hang during flashing BIOS if enabled Watch Dog Function.
19.[Fixes] Fixed 6240R and some refresh 4 serial CPU freq. can't reach the highest when enabling mwait.
20.[Fixes] Fixed BMC firmware revision may not correct in BIOS Setup.
21.[Fixes] Fixed System hang 0xB2 problem with some NVME device.
22.[Fixes] Fixed system will hang at POST code 0xA0 or 0xA2 when using non-support security NVME device and install Hyper-V with Windows 2019.
23.[Fixes] Fixed system hanging when plug AOC-MIBE6-m1C.
24.[Fixes] Fix "Configuration Address Source" always show "DHCP" in IPMI IPv6 page.
25.[Fixes] Failed to use SUM to change DCPMM setup item settins.
26.[Fixes] Fixed BIOS cannot detect riser card when install AOC-S100G-b2C after reboot system problem.
27.[Fixes] Update AMI EIP563137 to fix some BIOS items (like boot mode item) load default failure issue with some configurations (like with Micron M.2 or HGST SATA M.2)
28.[Fixes] Fixed UEFI SCT test found the "UEFI Compliant - Boot from iSCSI peripheral" fail.
29.[Fixes] Fixed system hang during flashing BIOS if enabled Watch Dog Function.
30.[Fixes] Fixed 6240R and some refresh 4 serial CPU freq. can't reach the highest when enabling mwait.
31.[Fixes] Fixed BMC firmware revision may not correct in BIOS Setup.
32.[Fixes] Fixed System hang 0xB2 problem with some NVME device.
33.[Fixes] Fixed system will hang at POST code 0xA0 or 0xA2 when using non-support security NVME device and install Hyper-V with Windows 2019.
34.[Fixes] Fixed system hanging when plug AOC-MIBE6-m1C.
35.[Fixes] Fix "Configuration Address Source" always show "DHCP" in IPMI IPv6 page.
36.[Fixes] Failed to use SUM to change DCPMM setup item settins.
37.[Fixes] Fixed BIOS cannot detect riser card when install AOC-S100G-b2C after reboot system problem.

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. Added support for Redfish feature.
6. Updated BIOS ACM 1.7.40 and SINIT ACM 1.7.48 PW.
7. 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).
8. Added support for Redfish functions.
9. Updated AMI label 5.14_PurleyCrb_0ACLA050 beta for IPU2020.1 PV.
10. Updated SPS_E5_04.01.04.381 from IPU 2020.1 PV.
11. Added setup item "HDD password prompt Control" to control "Hard-Drive Password Check" for enabling/disabling HDD password prompt window during POST.
12. Removed requirement to use Admin password for erasing TCG device.
13. Fixed problem of two CentOS boot items occurring in boot order if CentOS is installed in RAID 1 system.

3.2 (10/18/2019)
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 Skylake-SP and Cascade Lake-SP CPU 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.

3.1 (5/22/2019)

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. Updated Skylake-SP/Cascade Lake-SP CPU microcode.
5. Updated Intel BKCWW16 2019 PV PLR1.
6. Updated SPS_E5_04.01.04.296.0 from BKC WW16 2019.
7. Updated EIP467272 for AMI SA50069, SA50070.
8. Set SDDC Plus One or SDDC to disabled by default.
9. Updated SATA/sSATA RAID OPROM/EFI driver to VROC PreOS v6.1.0.1017.
10. Set ADDDC to enabled by default.
11. Fixed problem of UUID showing IPMI MAC incorrectly after disabling onboard LAN chip.
12. Temporarily fixed error for SKX (CLX) 4114 CPU memory training with Micron (18ASF2G72PDZ-2G6E1) RDIMM.
13. Fixed failure to boot into VMware OS when set to Maximum Performance even if Monitor/MWAIT is enabled.
14. 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.
15. Fixed problem of "?[1;31;40m" showing on POST screen when EFI driver is "Unhealthy".
16. Fixed inability to change IPv6 address or IPv6 Router1 IP address.

17. Set Leaky Bucket that can decrease one memory correctable error count within 2.15 minutes with threshold 512.
18. Fixed malfunction of workaround for GPU P2P low bandwidth.

3.0b (3/4/2019)
1. Added support for Purley Refresh platform.
2. Updated CPU microcodes from SRV_P_270.
3. Updated SINIT ACM 1.7.2 PW from BKC WW06 2019.
4. Updated SPS_E5_04.01.04.251.0 from Intel VIP Kit #130885.
5. Updated SATA RAID OPROM/EFI driver to RSTe PreOS v6.0.0.1024.
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 unused SPS ME "CUPS IIO" and "Volumetric Airflow" sensor.
9. Added support for Linux built-in utility efibootmgr.
10. Updated IPv6 router-related setup item string.
11. Reduced redundant reboot for offboard VGA switching.
12. Set NVDIMM ADR timeout to 600us.
13. 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.
14. Fixed problem of setup item "Quiet Boot" staying enabled after flashing BIOS with "Quiet Boot" disabled.
15. Modified UEFI network description to IPv4/IPv6 to follow Industry Standard.
16. Patched problem of system hanging at 0x94 when plugging in Nvidia Tesla T4 card.
17. Fixed inability of "Network Stack"-related items to get/change via SUM OOB method.

2.1 (7/6/2018)

1. Updated CPU microcode to address 'Spectre' derivatives (CVE-2018-3639 & CVE-2018-3640) security issue.
2. Updated BIOS ACM 1.3.7 and SINIT ACM 1.3.4.
3. Updated SPS 4.00.04.340 PL version.
4. Updated 5.12_PurleyCrb_0ACFD088 for Purley Skylake platform PLR7, BKC 2018 WW20.
5. Updated SATA RAID OPROM/EFI driver to RSTe PreOS v5.4.0.1039.
6. Added support for UEFI mode PXE boot of F12 hot key Net boot.
7. Added BIOS/ME downgrade check for SPS 4.0.4.340.
8. Added support for RFC3021.
9. Corrected help message for TPH BIOS setup items.
10. Displayed PPR setup item.
11. Added support for SATA FLR with enabled as default.
12. Added a patch to prevent reboot hang when installing AVAL APX-3224 card.
13. Added one event log to record that the event log is full.
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 Ctrl + Alt + Del causing system to hang after flashing BIOS.
16. Fixed inability of AFUWIN to keep VMD setting.
17. Fixed failure of WDT function.
18. Fixed inability of SMBIOS Type 40 to report SIOM card AOC-MTG-i2T/i4T information.
19. Fixed problem of system repeatedly rebooting when SIOM card AOC-MTG-i4T is plugged in.

2.0b (2/26/2018)

1. Updated 5.12_PurleyCrb_0ACFD085Beta for Purley Skylake platform PLR 4, BKC WW02.
2. Updated SPS 4.00.04.294 PLR 3.1 PV version.
3. Updated DMI CTLE value.
4. Updated re-driver for AOC-SLG3-2E4R.
5. Added setup item "SmcBusMasterEn" for enabling Parent bridge of the devices in the gSmcPciForceEnableBusMasterList.
6. Displayed setup item "ACS Control" to Enable/Disable PCIe Access Control Services Extended Capability, with Enabled as default.
7. Updated CPU microcode SRV_B_216 for Skylake-SP H0/M0/U0 stepping CPUs.
8. Updated BIOS version to 2.0b.
9. Updated BIOS ACM 1.3.5 and SINIT ACM 1.3.3.
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.
13. Changed RC default setting to upgrade POST Memory correctable error to uncorrectable error and map out the channel.
14. Fixed inability of BIOS to boot into OS with Intel P3608 PCIe NVMe drive installed.
15. Fixed issue with IPMI force boot.
16. Fixed issue of all commands requesting to be persistent.
17. Fixed malfunction of "SMBIOS Preservation" Disabled.
18. Fixed problem of SMC skipping first boot option in UEFI mode when retrying boot.
19. Fixed problem of the endpoint PCIe device having error bits in PCI Status or Device Status register.
20. Fixed inability to set memory policy.
21. Fixed inability to reset the system under DOS by pressing "Ctrl-Alt-Del" on USB keyboard when "Port 60/64 Emulation" is disabled.
22. Fixed failure of BIOS ECO ATT test case 306.
23. Disabled CPU2 IIO PCIe root port ACPI hot plug function.
24. Fixed inability of some CPUs to display correct microcode revision under BIOS setup menu.s