BIOS Release Notes Form

Product Name	**X11SSL(-F)/X11SSM**
Release Version	**2.6**
Release Date	**6/12/2021**
Build Date	**6/12/2021**
Previous Version	**2.5**
Update Category	**Recommended**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Changed BIOS revision to 2.6.** **2. Updated Skylake-S R0/S0 stepping CPU beta microcode M36506E3_000000EA and Kabylake-S B0 stepping CPU beta microcode M2A906E9_000000EA for INTEL-SA-00464 Security Advisory to address CVE-2020-24511 (5.6, Medium) and CVE-2020-24512 (2.8, Low) security issues.** **3. Updated SPS 4.01.04.306 PC for 2021.1 IPU.**
New features	**N/A**
Fixes	**N/A**

Release Notes from Previous Release(s)

2.5 (11/26/2020)

1. Changed BIOS revision to 2.5.
2. Updated SPS 4.01.04.204 for IPU 2020.2 for INTEL-SA-00391 Security Advisory to address CVE-2020-8752 (9.4, Critical), CVE-2020-8753 (8.2, High), CVE-2020-12297 (8.2, High), CVE-2020-12304 (8.2, High), CVE-2020-8745 (7.3, High), CVE-2020-8744 (7.2, High), CVE-2020-8705 (7.1, High), CVE-2020-8750 (7.0, High), CVE-2020-12303 (7.0, High), CVE-2020-12354 (6.7, Medium), CVE-2020-8757 (6.3, Medium), CVE-2020-8756 (6.3, Medium), CVE-2020-8760 (6.0, Medium), CVE-2020-12355 (5.3, Medium), CVE-2020-8751 (5.3, Medium), CVE-2020-8754 (5.3, Medium), CVE-2020-8761 (4.9, Medium), CVE-2020-8747 (4.8, Medium), CVE-2020-8755 (4.6, Medium), CVE-2020-12356 (4.4, Medium), CVE-2020-8746 (4.3, Medium), and CVE-2020-8749 (4.2, Medium) security issues.
3. Updated MRC Version 4.1.1.5 for IPU 2020.2.
4. Updated Skylake-S R0/S0 stepping CPU microcode M36506E3_000000E2 and Kabylake-S B0 stepping CPU microcode M2A906E9_000000DE for IPU 2020.2 for INTEL-SA-00389 Security Advisory to address CVE-2020-8694 (5.6, Medium) and CVE-2020-8695 (5.3, Medium) security issues.

2.4 (6/2/2020)

1. Changed BIOS revision to 2.4.
2. Updated Skylake-S R0/S0 stepping CPU beta microcode M36506E3_000000DC and Kabylake-S B0 stepping CPU beta microcode M2A906E9_000000D6 for IPU2020.1 and INTEL-SA-00295 Security Advisory to address CVE-2020-0542 (7.8, High), CVE-2020-0532 (7.1, High), CVE-2020-0538 (7.5, High), CVE-2020-0534 (7.5, High), CVE-2020-0541 (6.7, Medium), CVE-2020-0533 (7.5, High), CVE-2020-0537 (4.9, Medium), CVE-2020-0531 (6.5, Medium), CVE-2020-0535 (5.3, Medium), CVE-2020-0536 (5.5, Medium), CVE-2020-0545 (4.4, Medium), CVE-2020-0540 (5.3, Medium), CVE-2020-0566 (7.3, High), CVE-2020-0539 (3.3, Low), CVE-2020-0586 (7.3, High), CVE-2020-0594 (9.8, Critical), CVE-2020-0595 (9.8, Critical), CVE-2020-0596 (7.5, High), CVE-2020-8674 (4.3, Medium), and CVE-2020-0597 (6.5, Medium) security issues.
3. Updated MRC Version 4.1.1.4.
4. Updated SPS 4.01.04.109 PLR version for IPU 2020.1.
5. Fixed problem of system hanging at 0x92 when installing Avago 9460-16i with EFI mode.

2.3 (11/26/2019)

1. Changed BIOS revision to 2.3.
2. Updated SPS 4.01.04.088 PLR version for INTEL-SA-00241 Security Advisory to address CVE-2019-11090 (6.8, Medium), CVE-2019-11088 (7.5, High), CVE-2019-0165 (4.4, Medium), CVE-2019-0166 (5.9, Medium), CVE-2019-0168 (4.6, Medium), CVE-2019-0169 (9.6, Critical), CVE-2019-11086 (3.5, Low), CVE-2019-11087 (6.4, Medium), CVE-2019-11101 (4.4, Medium), CVE-2019-11100 (6.1, Medium), CVE-2019-11102 (4.1, Medium), CVE-2019-11103 (7.3, High), CVE-2019-11104 (7.3, High), CVE-2019-11105 (7.9, High), CVE-2019-11106 (4.4, Medium), CVE-2019-11107 (5.3, Medium), CVE-2019-11108 (2.3, Low), CVE-2019-11110 (4.1, Medium), CVE-2019-11097 (7.3, High), CVE-2019-0131 (7.1, High), CVE-2019-11109 (4.4, Medium), CVE-2019-11131 (7.5, High), CVE-2019-11132 (8.4, High), and CVE-2019-11147 (8.2, High) security issues.
3. Updated SI 4.1.1.3 for INTEL-SA-00260 Security Advisory to address CVE-2019-0154 (6.5, Medium) security issue.
4. Updated Skylake-S R0/S0 stepping CPU microcode M36506E3_000000D6 and Kabylake-S B0 stepping CPU microcode M2A906E9_000000CA for INTEL-SA-00219 Security Advisory to address CVE-2019-0117 (6.0, Medium) security issue, INTEL-SA-00289 Security Advisory to address CVE-2019-11157 (7.9, High) security issue, and INTEL-SA-00242 Security Advisory to address CVE-2019-11112 (8.8,

High), CVE-2019-0155 (8.8, High), CVE-2019-11111 (7.3, High), CVE-2019-14574 (6.5, Medium), CVE-2019-14590 (6.5, Medium), CVE-2019-14591 (6.5, Medium), CVE-2019-11089 (5.9, Medium), and CVE-2019-11113 (4.0, Medium) security issues.
5. Updated Kaby Lake BIOS ACM 1.6.0 and SINIT ACM 1.7.4 for INTEL-SA-00220 Security Advisory to address CVE-2019-0123 (8.2, High) and CVE-2019-0124 (8.2, High) security issues and INTEL-SA-00240 Security Advisory to address CVE-2019-0151 (7.5, High) and CVE-2019-0152 (8.2, High) security issues.
6. Updated Secure Boot Key.
7. Implemented security update for INTEL-SA-00254 Security Advisory to address CVE-2019-0185 (6.0, Medium) security issue.

2.2a (5/24/2019)

1. Updated Intel CPU microcode from DT_P_183 for INTEL-SA00233 Security Advisory to address CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, and CVE-2019-11091 security issues.
2. Updated EIP419363 to ensure DCI Policy is "Disabled" for INTEL-SA-00127, EIP412144 for [SA50044] USRT Mantis vulnerabilities, EIP387724 for Ofbd Meud Security vulnerabilities, and EIP422042 for CPU microcode downgrade attack vulnerability.
3. Updated Greenlow Refresh Initialization Code PV PLR5 Hotfix1 version 4.1.1.1 for INTEL-SA-00223 Security Advisory to address CVE-2019-0119, CVE-2019-0120, and CVE-2019-0126 security issues.
4. Contained SPS 4.01.04.054 PLR version for security vulnerability INTEL-SA-00213 to address CVE-2019-0089, CVE-2019-0090, CVE-2019-0086, CVE-2019-0091, CVE-2019-0092, CVE-2019-0093, CVE-2019-0094, CVE-2019-0096, CVE-2019-0097, CVE-2019-0098, and CVE-2019-0099 security issues.
5. Changed BIOS revision to 2.2a.
6. Updated Kaby Lake BIOS ACM 1.5.0 and SINIT ACM 1.6.0.
7. Updated EIP393007 & EIP411789 for TPM vulnerability when resuming S3.
8. Updated SATA RAID OPROM/EFI driver to RSTe PreOS v4.7.0.1017.
9. Updated VBIOS and VGA EFI Driver to 1.09 to fix ASpeed CVE-2019-6260 security issue.
10. Updated valid range of IPMI setup item VLAN ID to 1-4094.
11. Added support for RFC4122 UUID format feature to set RFC4122 encoding from build time produced by IPMICFG 1.29 tool or newer.
12. Fixed problem of BIOS always retrying boot when Re-Try Boot is Disabled.
13. Fixed inability to disable SMBIOS preservation for recovery.
14. Fixed inability to log CECC events in IPMI event log when METW = 0.

2.2 (5/23/2018)

1. Changed BIOS revision to 2.2.
2. Updated CPU microcode to address CVE-2018-3639 and CVE-2018-3640.
3. Updated Kaby Lake BIOS ACM 1.4.0 and SINIT ACM 1.3.0.
4. Enhanced ability to enter setup menu without password when system only has Administrator password.
5. Fixed problem of Afu /O command clearing SMC SMBIOS region ($SMC).
6. Implemented workaround for problem of IP displaying 0.0.0.0 information the first time AC powers on BMC.
7. Fixed problem of the system hanging when trying to create virtual driver on LSI3108 storage card under BIOS setup.
8. Fixed missing reminding string "iKVM doesn't support add-on VGA device..." when VGA is plugged in & "Primary Display"=="PEG".

2.1a (03/07/2018)

1. Updated CPU microcode to address 'Spectre' variant 2 (CVE 2017-5715) security issue.
2. Changed BIOS revision to 2.1a.
3. Added Ramaxel JEDEC Manufacturer ID to support Ramaxel memory.
4. Added AOC-SLG3-2M2 1.01 into NVMe table for auto bifurcation.
5. Added support to speed the memory up to 2667Mhz.
6. Added support for UEFI mode PXE boot via F12 hot key Net boot.
7. Added support for SUM to display SGX-related items.
8. Fixed issue with IPMI force boot.
9. Fixed inability to load Broadcom SAS3008 configuration utility.
10. Fixed problem of system not showing correct manufacturer name or product name when IPMI without FRU1 is programmed.
11. Fixed failure of ATT BIOS ECO test case 237.
12. Fixed problem of SGX resetting to default value if using SUM to change SGX items after BIOS update.

2.1 (12/11/2017)

1. Changed BIOS revision to 2.1 for INTEL-TA-201710-003.
2. Updated SATA RAID OPROM/EFI driver to RSTe PreOS v4.7.0.1014.
3. Updated DT_P_140 for Kaby Lake-S B0 stepping MCU M2A906E9_0000007C and Skylake-S R0/S0 stepping MCU M36506E3_000000C2.
4. Fixed problem of ACPI Exception: AE_NOT_FOUND occurring.

2.0c (10/6/2017)
1. Changed BIOS revision to 2.0c.
2. Updated Greenlow Refresh Initialization Code PV PLR3 Version 4.1.0.8.
3. Updated DT_P_129 for Kaby Lake-S B0 stepping microcode M2A906E9_00000070.
4. Added a workaround to clear onboard LAN and slot device's UR and CE status.
5. Updated Skylake-S R0/S0 stepping microcode M36506E3_000000BE.
6. Added "SMBIOS Preservation" Enabled/Disabled item for flash recovery.
7. Added AOC-SLG3-2M2 into NVMe table for auto bifurcation.
8. Added support for NVMe Firmware Source BIOS setup item.
9. Updated SPS 4.01.04.054 PLR version for security vulnerabilities.
10. Corrected the slot number for PEG/PCH slot.
11. Fixed inability of Windows PXE server to install OS successfully after IPMI forces PXE to boot.
12. Fixed problem of SPS NM command "Set Max allowed CPU P-state/T-state" working abnormally under OS.

2.0b (7/28/2017)
1. Changed BIOS revision to 2.0b.
2. Updated Intel Kaby Lake RC/SI package 4.1.0.6 PLR2.
3. Updated DT_P_123 for Kaby Lake-S B0 stepping microcode M2A906E9_0000005E and Skylake-S R0/S0 stepping MCU M36506E3_000000BA.
4. Set enabled SATA Hot Plug as default.
5. Added support for new Micron ECC_On_Die chip(I-Die).
6. Displayed SGX-related items.
7. Updated Kaby Lake BIOS/SINIT ACM 1.2.0.
8. Added SumBbsSupportFlag into DAT file.
9. Added TPM PCR measurements for PCR[1], PCR[2], and PCR[6].

10. Removed the "Unrecoverable Media control failure" event log from BMC.
11. Added a workaround to clear onboard LAN device UR, CE status.
12. Fixed problem of valid bit being checked before IPMI CMOS clear flag.
13. Fixed system reset or hanging after Watchdog function is enabled during BIOS update.
14. Fixed issue of SUM TC306 and TC317 failing in certain configuration cases.
15. Fixed inability of the system to enter "Recovery mode" automatically if BIOS ACPI table in the Main Block is corrupted.
16. Fixed issue of system halting at 0xB2 when disabling JPG1.
17. Fixed incorrect CECC DIMM location being reported in BMC SEL log.
18. Fixed problem of IPMI device _CRS being reported as 0xca2 or 0xca3.
19. Fixed problem of "file size is zero" error occurring when using SUM in-band command "GetCurrentBiosCfg".
20. Fixed inability to find correct Memory CECC DIMM location through SD5.
21. Fixed problem of "No DIMM Information" showing for Memory CECC in Event log of BIOS Setup.
22. Fixed problem of recovery from JBR1/FFS Check hanging at 0x90.

2.0a (3/09/2017)

1. Changed BIOS revision to 2.0a.
2. Updated Intel RC/SI to 4.1.0.2.
3. Updated SPS to 4.1.3.22 PV release.
4. Added "Kaby Lake" to "System Agent Bridge Name".
5. Updated DT_P_119 for Skylake R0 stepping microcode M36506E3_000000B2.
6. Updated RSTe PreOS 4.6.0.1018.
7. Set "PCI AER Support" setup item to display to OOB.
8. Added AMI EarlyConsoleOut_02 module and SmcEarlyConsoleStatus from SVN#2572.
9. Fixed problem of system hanging at 0x35 with Skylake CPU when JBR1 is enabled after a flash failed.
10. Fixed problem of system hanging when installing an add-on card that contains non-SMC format VPD data.
11. Fixed operation of COM1 console redirection default setting (disabled) in MFG mode.
12. Fixed problem of Greenlow CPUs not working at minimum CPU frequency (800 MHz) with a non-ACPI aware OS (e.g., DOS and EFI Shell) when setting "Boot Performance Mode" to "Power Saving" in the BIOS setup menu.
13. Fixed problem of Multi event time count not following the specifications.
14. Fixed issue of power button not being reported in the ACPI table when set to "4 Seconds Override" in BIOS.
15. Enhanced code for no NM support to prevent CPU from running at power-saving speed.
16. Fixed problem of SMBIOS Type 17 Manufacturer being incorrect when installing memory that has an unknown manufacturer to display as “Undefined”.

2.0 (01/06/2017)
1. Changed BIOS revision to 2.0 for Kaby Lake (Greenlow Refresh) CPU support.
2. Updated Kernel to 5.11_VEB_1ATYX009 and MRC 3.9.0.6.
3. Updated the codes for [ACPI PCI _DSM:function7].
4. Updated DT_P_116 for Kabylake-S ucode M22906E9_00000047_00000048.
5. Fixed problem of using AMIBCP to disable display of boot procedure messages failing on non-F platform.
6. Fixed problem of boot order priority in submenu group not working properly if selecting "Save Changes" and then selecting "Save Changes and Reset" in setup.

7. Implemented CPU maximum performance function.
8. Fixed problem of system hanging at 0x35 when enabling JBR1.
9. Fixed problem of system hanging at POST when using SUM to change BIOS settings without reboot and flashing BIOS at the same time.
10. Updated SPS to 4.1.3.19 PC release.
11. Patched inability of CTRL+HOME to work via console.
12. Synced up BIOS revision of setup and POST message with SMBIOS Type 0.
13. Fixed TC320 issue.
14. Reset BIOS configuration via IPMI CMOS clear flag.
15. Fixed problem of boot override menu showing blank item when changing boot mode to UEFI or Legacy.
16. Updated SMCI default key for Secure Boot.
17. Fixed issue of system booting to UEFI boot devices when there is no matching type found in boot list.
18. Added support for Intel LAN 82599 (1-port, DID=1557) to AOC report and UEFI PXE/iSCSI boot.
19. Set above 4G MMIO resource to 128GB.
20. Updated Aspeed VBIOS to v1.02.07.
21. Updated AMI EIP#268836 to fix problem of system looping in CPU SMM mode after running BMC firmware upgrade loop test for over 24 hours.
22. Added WDT timeout value selection.
23. Fixed problem of the FID table being x.x0 when revision is x.x.
24. Added support for VPD info and AssetInfo in SMBIOS type 40.
25. Changed PCN from 0xC0 to 0xC1 for 2133Mhz and SPD revision 1.1 support.
26. Set the CSM support to be disabled when Secure boot control is enabled.
27. Fixed problem of SATA Latency Tolerance Reporting (LTR) workaround not programming correctly.
28. Displayed USB Configuration setup page.
29. Fixed problem of Security Device Support hiding after disabling Security Device Support and rebooting.
30. Fixed failure of SUM test with duplicated strings.
31. Displayed Execute Disable Bit setup item.
32. Updated SUM Feature Flag specifications to 1.4.
33. Displayed SATA "Aggressive LPM Support" setup option and set disabled as default.
34. Fixed problem of system hanging in BIOS setup when the SMBIOS event log is full.
35. Fixed incorrect VPD header version in VPD data.
36. Fixed incorrect SMBIOS Type 17 serial number.
37. Corrected SMBIOS help string typo.
*38. Changed logo resolution from 800*600 to 1024*768.*
42. Added check flash package flag that adds a flag for BIOS check.
40. Enabled OA1_SUPPORT to fix inability to modify OEM Data by AMIBCP.exe.
41. Fixed problem of memory UCE occurring in system after toggling "PCI PERR/SERR Support" setting with full DIMM population.
42. Fixed problem of "X2APIC Opt Out" item always being hidden.
43. Fixed problem of system hanging at 0x35 with Skylake CPU when JBR1 is enabled after flash failure.

1.0b (12/29/2015)

1. Updated SPS firmware to 4.0.3.89.
2. Updated Intel Skylake TXT ACM R1.3.
3. Added Skylake Platforms Silicon Initialization Code 1.6.0.1, Bug Name 2.

4. Added Skylake Platforms Silicon Initialization Code 1.6.0.1, Bug Name 3.
5. Displayed SGX setup item and set Enable as default.
6. Enabled use of BIOS setup menu item to enable/disable Win7 USB Keyboard/Mouse support.
7. Updated Skylake-S R0 stepping ucode M36506E3_0000006A.
8. Added BMC VLAN items to BIOS setup.
9. Updated the GPNV memory error event structure.
10. Updated TCG2 module to label TCG2_07.
11. Fixed problem of system hanging with Broadcom Lan card (BCM 95708A0804F).
12. Added default value for Serial Ports.
13. Set disabled CECC error reporting as default.
14. Hid the "SW Guard Extensions (SGX)" item for SUM.
15. Fixed incorrect date and time of event log.
16. Fixed problem of system randomly hanging at post code 0xad while booting to UEFI Red Hat 6.5 x64 OS.
17. Fixed problem of DMI being lost after clearing event log.
18. Fixed inability to insert OA3 and clear OA2 backup area.
19. Fixed problem of HDD dropping when enabling Above 4G decoding.
20. Added support for PROCHOT out function when CPU overheat alarm is triggered.
21. Fixed issue of low IB bi-direction performance.