BIOS Release Notes Form

Product Name	**X11SSW-(4)TF**
Release Version	**2.8**
Release Date	**9/15/2022**
Build Date	**9/15/2022**
Previous Version	**2.7**
Update Category	**Recommended**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Changed BIOS revision to 2.8.** **2. Updated the DBX file to fix the Secure Boot Bypass issue.** **3. Updated EIP#696788, 694328 for IPU IPU2022.3 PV Sample Code 006.98 to address Intel-SA00688: CVE-2022-26837 (7.5 High).** **4. Updated SPS 4.01.04.700 for IPU 2022.3 to address Intel-TA00610: CVE-2022-29466 (7.3 High) and INTEL-SA-00669 Security Advisory to address CVE-2022-26074 (6.0, Medium) security issue.**
New features	**N/A**

Fixes	**N/A**

Release Notes from Previous Release(s)

2.7 (12/8/2021)

1. *Changed BIOS revision to 2.7.*
2. *Updated SPS 4.01.04.400 PC for 2021.2 IPU.*
3. *Updated Skylake-S R0/S0 stepping CPU beta microcode M36506E3_000000EC. Updated Kabylake-S B0 stepping CPU beta microcode M2A906E9_000000EC. For INTEL-SA-00532 Security Advisory to address CVE-2021-0127(5.6, Medium) security issue.*
4. *Updated MRC Version 4.1.1.6. For INTEL-SA-00562 Security Advisory to address CVE-2021-0157(8.2, High) and CVE-2021-0158(8.2, High) security issues. 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. *Updated SINIT ACM to v1.9.1. For INTEL-SA-00562 Security Advisory to address CVE-2021-0157(8.2, High) and CVE-2021-0158(8.2, High) security issues. 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.*

2.6 (06/15/2021)

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.

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.
8. Fixed missing OEM string of SMBIOS type 11.

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 (5/24/2018)

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 (3/2/2018)

1. Updated DT_B_128 for Kaby Lake-S B0 stepping CPU microcode M2A906E9_00000084 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 support to speed the memory up to 2667Mhz.
5. Added support for UEFI mode PXE boot via F12 hot key Net boot.
6. Added support for SUM to display SGX-related items.
7. Updated SATA RAID OPROM/EFI driver to RSTe PreOS v4.7.0.1014 (RSTe SATA 4.7.0.1069 and NVMe 4.7.0.2063).
8. Updated SUM BIOS setup change before setup/logo.
9. Fixed inability to load Broadcom SAS3008 configuration utility.
10. Fixed issue with IPMI force boot.

11. Fixed problem of system not showing correct manufacturer name or product name when IPMI without FRU1 is programmed.
12. Fixed failure of ATT BIOS ECO test case 237.
13. Fixed problem of SGX resetting to default value if using SUM to change SGX items after BIOS update.
14. Changed SGX EpochUpdate and EpochToFactory items' behavior of resetting to 0 if using SUM to set two items.
15. Changed "primary display" = "PCIe" to follow setup template.

2.1 (12/11/2017)

1. Changed BIOS revision to 2.1.
2. Updated Kaby Lake-S B0 stepping MCU M2A906E9_0000007C.