BIOS Release Notes Form

Product Name	**X11SSA-F/X11SSi-LN4F**
Release Version	**2.5**
Release Date	**11/25/2020**
Build Date	**11/25/2020**
Previous Version	**2.4**
Update Category	**Critical**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Updated SPS 4.01.04.204 for IPU 2020.2 Intel-TA-00391: CVE-2020-8705 (High, 7.1) security issue.** **2. Updated MRC Version 4.1.1.5 for IPU 2020.2.** **3. 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-TA-00381: CVE-2020-8696 (Low, 2.5) and Intel-TA-00389: CVE-2020-8694 (Medium, 5.6), CVE-2020-8695 (Medium, 5.3) security issues.**
New features	**N/A**
Fixes	**N/A**

Release Notes from Previous Release(s)

2.4 (6/3/2020)

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.

2.3 (12/12/2019)

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. Added IB and LSI HBA device report for 0x3A command.

2.2a (5/23/2019)

1. Updated Intel CPU microcode from DT_P_183 for INTEL-SA00233 Security Advisory.
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.
5. Updated Kaby Lake BIOS ACM 1.5.0 and SINIT ACM 1.6.0.
6. Updated EIP393007 & EIP411789 for TPM vulnerability when resuming S3.
7. Updated SATA RAID OPROM/EFI driver to RSTe PreOS v4.7.0.1017.
8. Updated VBIOS and VGA EFI Driver to 1.09 to fix ASpeed CVE-2019-6260 security issue.
9. Updated valid range of IPMI setup item VLAN ID to 1-4094.
10. Added support for RFC4122 UUID format feature to set RFC4122 encoding from build time produced by IPMICFG 1.29 tool or newer.
11. Fixed problem of BIOS always retrying boot when Re-Try Boot is Disabled.
12. Fixed inability to disable SMBIOS preservation for recovery.
13. Fixed inability to log CECC events in IPMI event log when METW = 0.

2.2 (5/23/2018)

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

2.1a (02/12/2018)

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. Added support for UEFI mode PXE boot via F12 hot key Net boot.
3. Added support for SUM to display SGX-related items.
4. Added AOC-SLG3-2M2 1.01 into NVMe table for auto bifurcation.
5. Added Ramaxel JEDEC Manufacturer ID to support Ramaxel memory.
6. Fixed inability to load Broadcom SAS3008 configuration utility.
7. Fixed issue of all commands requesting to be persistent.
8. Fixed issue with IPMI force boot.

2.1 (12/10/2017)

1. Updated DT_P_140 for Kaby Lake-S B0 stepping MCU M2A906E9_0000007C and Skylake-S R0/S0 stepping MCU M36506E3_000000C2.
2. 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).
3. Fixed problem of ACPI Exception: AE_NOT_FOUND occurring.

2.0c (10/7/2017)

1. Updated Greenlow Refresh Initialization Code PV PLR3 Version 4.1.0.8.
2. Updated DT_P_129 for Kabylake-S B0 stepping microcode M2A906E9_00000070.
3. Updated Skylake-S R0/S0 stepping microcode M36506E3_000000BE.
4. Fixed problem of recovery from JBR1/CTRL+HOME/FFS Check all hanging at 0x90.
5. Added AOC-SLG3-2M2 into NVMe table for auto bifurcation.
6. Added support for NVMe Firmware Source BIOS setup item.
7. Added "SMBIOS Preservation" Enabled/Disabled item for flash recovery.
8. Updated SPS 4.01.04.054 PLR version for security vulnerabilities.
9. Fixed problem of "No DIMM Information" showing for Memory CECC in Event log of BIOS Setup.
10. Fixed inability to get correct Memory CECC DIMM location by SD5.
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.