BIOS Release Notes Form

Product Name	**X11SRM-(V)F**
Release Version	**2.5**
Release Date	**2/15/2022**
Build Date	**2/15/2022**
Previous Version	**2.4**
Update Category	**Critical**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Changed BIOS version to 2.5.** **2. Updated RC code to 3362.D01 for GlacierFallsWS IPU 2021.2. For INTEL-TA-00525 Security Advisory to address CVE-2021-0144(7.5, High), INTEL-TA-00562 Security Advisory to address CVE-2021-0157(8.2, High) INTEL-TA-00527 Security Advisory to address CVE-2021-0156(7.5, High).** **3. Updated Intel Corporate ME FW to version ME 11.12.90.1962.** **4. Updated Skylake Microcode MB750654_02006C0A, MB750656_0400320A, MBF50657_0500320A for INTEL-TA-00532 2021.2 IPU to address CVE-2021-0127 (5.6 Medium).** **5. Enabled "CUSTOMIZED_SECURE_BOOT_DEPLOYMENT_SETUP" to support Secure Boot deployment in BIOS setup menu.**

New features	**N/A**
Fixes	**1. Fixed when install UEFI RedHat/CentOS/Fedora/ubuntu there are two boot devices in the boot order.** **2. Fixed when trigger the ECC/UECC then will cause system hang up.**

Release Notes from Previous Release(s)

2.4 (6/14/2021)

1. Updated the BIOS version to 2.4.
2. Updated RC code to 2522.D00 for GlacierFallsWS IPU 2021.1.
3. Updated Skylake microcodes MB750654_02006B06, MBF50656_04003102, and MBF50657_05003102 for INTEL-TA-00464 2021.1 IPU to address CVE-2020-24511 (5.6, Medium) security issue.
4. Updated Intel Client ME to version ME 11.12.86.1877 for INTEL-TA-00459 Security Advisory to address CVE-2020-24506 (4.4, Medium), CVE-2020-8704 (6.7, Medium), and CVE-2020-24507 (6.0, Medium) security issues.
5. Displayed the memory PPR Type item.
6. Updated Intel RSTe/VROC RAID Option UEFI driver to 7.0.0.2086.
7. Added the CPU core limit items to the BIOS setup menu.
8. . Fixed failure of the re-try boot function.
9. Fixed issue with Intel Turbo Boost Max Technology 3.0 yellow ban.

2.3 (10/19/2020)

1. Updated the BIOS version to 2.3.
2. Updated Skylake microcodes MB750654_02006A08 and MBF50657_05003003 for INTEL-SA-00358 Security Advisory to address CVE-2020-0590 (7.7, Height), 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) security issues.
3. Updated ME corporate firmware 11.12.80.1734 for INTEL-TA-00391 Security Advisory to address CVE-2020-8752 (9.4, Critical), CVE-2020-8753 (8.2, High), CVE-2020-12297 (8.2, High), CVE-2020-8745 (7.3, High), CVE-2020-8705 (7.1, High), CVE-2020-12303 (7.0, High), 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) security issues.
4. Updated AHCI_24, Recovery_19, GpnvErrorLogging_17, and NVRAM_22 for AMI SA50077 Q4 2019 Security Review.
5. Added the CPU core limit items to the BIOS setup menu.
5. Fixed issue of system resetting when using VGA card Tesla P100 or K80.
6. Fixed problem of system hanging on CP: B6h when plugging in RTX 2080 and P100, then clearing CMOS.

2.2 (9/3/2020)

1. Updated the BIOS version to 2.2.
2. Updated SecureBoot module to label 32 for AMI SA-50085 Grub Bootloader vulnerability to address CVE-2020-10713 (8.2, high) security issue.
3. Updated ME corporate 11.12.79.1722 for INTEL-SA-00404 Security Advisory to address CVE-2020-8758 (9.8, Critical) security issue.
4. Added "Auto" item to the Above 4G option and set default to "Auto".
5. Fixed inability of SUM to dump the setup items of Advanced/Chipset Configuration/North Bridge/IIO Configuration page.

2.1 (6/20/2020)

1. Updated the BIOS version to 2.1.

2. Enhanced support for Glacier Falls WS Turbo Boost 3.0 feature.
3. Updated ME 11.12.77.1664 for 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.
4. Set "No memory DIMM detected, install memory DIMMs" string to display when there is no DIMM in a slot.
5. Added ACS control item to Advanced/Chipset Configuration/North Bridge/IIO Configuration/Intel VT for Directed I/O (VT-d) page.
6. Updated RC code to 1524.D00 for GlacierFallsWS IPU 2020.1.
7. Updated Intel RSTe RAID Option ROM/UEFI Driver to 6.3.0.1005 and VMD to 6.2.0.1034.
8. Added back the "NVMe Configuration" items.
9. Updated Skylake microcode MB750654_02006906 for INTEL-SA-00329 Security Advisory to address CVE-2020-0548 (2.8, Low) and CVE-2020-0549 (6.5, Medium) security issues and Cascade Lake microcodes MBF50657_05002F01 and MBF50656_04002F01 for INTEL-SA-00329 Security Advisory to address CVE-2020-0548 (2.8, Low) and CVE-2020-0549 (6.5, Medium) security issues.
10. Fixed failure of system to boot when plugging in K80.
11. Fixed problem of the SMBIOS type 17 manufacturing date being empty.
12. Fixed problem of the system hanging up when EuP mode is enabled then CMOS is cleaned.
13. Fixed failure of SUM TC: 210/304/408 test.
14. Fixed problem of the system hanging up at CP: 3Bh when plugging in 5 VGAs to the system, including one VGA in the PCH.
15. Removed the "System Firmware Error (POST ERROR)" error log from BMC and "EFI 01030006" from BIOS event log.
16. Corrected DMI Type2 when the PCD product name is shorter than the FRU1 product name.

2.0a (12/12/2019)

1. Changed BIOS version to 2.0a.
2. Modified the IIO string in the BIOS setup menu.
3. Rolled back SINIT ACM from BSF_GCF_SINIT_v_1_3_54_20191029_KBL_PW_signed to BASINFALLS_SINIT_v1_3_1_20170613_KBL_PW_signed.
4. Fixed inability of onboard NVMe socket to use IPMI Web to eject problem.
5. Fixed inability to use IPMI Web to eject when plugging in NVMe add-on card (AOC-SLG3-4E4).
6. Fixed failure of user password to clear after clearing administrator password.
7. Fixed ability to enter Setup Menu if ADMIN password is set after pressing "Enter".
8. Fixed failure of IPMI web setting to sync with BIOS IPMI page.
9. Fixed problem of recovery page title showing as "Main" and recovery page disappearing when moved to another page under recovery mode.
10. Fixed problem of system hanging up in CP: A2h when running PCH on/off test.

2.0 (10/31/2019)

1. Added support for Glacier Falls CLX-W CPU.
2. Updated PCIe module in the Glacier Falls platform.
3. Updated the USB module in the Glacier Falls platform.
4. Updated the TPM module in the Glacier Falls platform.

5. Updated the ESA setup menu module in the Glacier Falls platform.
6. Updated the console redirection module in the Glacier Falls platform.
7. Updated the serial port function in the Glacier Falls platform.
8. Updated the power policy setting in the Glacier Falls platform.
9. Updated the SATA module function in the Glacier Falls platform.
10. Updated the SMC OC module in the Glacier Falls platform.
11. Added SMC Password style in the Glacier Falls Projects.
12. Added AER and MCE items.
13. Updated ME 11.12.00.1622.
14. Added "SMBIOS Preservation" Enabled/Disabled item for flash recovery.
15. Updated VROC VMD driver, RSTe UEFI driver, and Legacy ROM to 6.2.0.1034.
16. Implemented prompt message at post screen when entering BIOS recovery mode for the platform to support early video.
17. Updated Skylake microcode MB750654_02000065 for INTEL-SA-00271 Security Advisory to address CVE-2019-11139 (5.8, Medium) security issue and Cascade Lake microcodes MBF50656_0400002C & MBF50657_0500002C for INTEL-SA-00270 Security Advisory to address CVE-2019-11135 (6.5, Medium) security issue.
18. Updated Basin Falls BIOS ACM and SINIT ACM to PW version.
19. Changed the maximum value of Memory Frequency to 2933 in Memory page.
20. Fixed inability of system to boot when setting BIOS setup menu CSM to disabled.
21. Removed LAN2 GBe definition since LAN1 and LAN2 use the same UEFI driver.
22. Fixed problem of the "Storage Option ROM/UEFI Driver" being masked when using AMI SCE tool to dump to BIOS setup items.
23. Fixed problem of non-support status returning when using AFU tool to clean event log.
24. Fixed inability to change the VGA priority by SMC Option ROM control function.
25. Set message to show in the onboard VGA output when changing VGA priority to add-on card.
26. Added item "Storage Option ROM/UEFI Driver" to Advanced/SATA and RST Configuration page.
27. Fixed inability to load VMD driver when enabling VMD ports under "Intel VMD Technology" menu.
28. Fixed failure of serial port when using PC Check tool test.
29. Enabled the PROCHOT pin as BIDIRECTIONAL by default to support processor hot feature.
30. Fixed malfunction of the Watchdog.

1.2b (4/29/2019)

1. Updated ME 11.11.60.1561 for INTEL-SA-00185 Security Advisory to address CVE-2018-12188, CVE-2018-12189, CVE-2018-12190, CVE-2018-12191, CVE-2018-12192, CVE-2018-12199, CVE-2018-12198, CVE-2018-12208, CVE-2018-12200, CVE-2018-12187, CVE-2018-12196, CVE-2018-12185.
2. Updated VROC VMD driver, RSTe UEFI driver, and Legacy ROM to 6.1.0.1017.
3. Added AER and MCE items.
4. Updated ME 11.11.65.1590 for INTEL-SA-00213 Security Advisory to address CVE-2019-0089, CVE-2019-0090, CVE-2019-0086, CVE-2019-0091, CVE-2018-12192, CVE-2018-12199, CVE-2018-12198, CVE-2018-12208, CVE-2018-12200, CVE-2018-12187, CVE-2018-12196, CVE-2018-12185.
5. Exposed “Correctable Error Threshold” in Advanced/Chipset/North Bridge/Memory/RAS page.
6. Updated Skylake U-0 stepping CPU microcode.
7. Fixed problem of system boot working slowly into PXE.
8. Fixed inability of NMI to trigger BSOD.
9. Fixed the range of BIOS setup menu item VLAN ID from 1 to 4094.

1.2a (2/18/2019)

1. Updated BIOS version to 1.2a.
2. Updated SkyLake H-0/M-0/U-0 stepping CPU microcode MB750654_02000057.
3. Updated SMBIOS type 11 OEM String size to 50 bytes.
4. Updated ME to 11.11.60.1561 for INTEL-SA-00185 Security Advisory security issue.
5. Updated Intel RSTe RAID Option ROM/UEFI Driver to 5.5.0.1028.
6. Updated BasinFalls RC to 1.1.7.
7. Implemented prompt message at post screen when entering BIOS recovery mode for the platform to support early video.
8. Added support for RFC4122 UUID format feature to set RFC4122 encoding from build time produced by IPMICFG 1.29 tool or newer.
9. Fixed inability of system to boot when using Intel W-2195 CPU.
10. Fixed problem of PCR#1 value changing during Legacy boot with TPM 2.0 when Measure_Smbios_Tables is disabled.
11 Fixed inability to enable SR-IOV when using the 82599 add-on card.
12. Fixed problem of boot menu losing HDD when plugging in TPM 1.2.

1.2 (9/19/2018)

1. Updated CPU microcode to address 'Spectre' derivatives (CVE-2018-3639 & CVE-2018-3640) security issue.
2. Set VGA device IO resources assignment to be skipped when system is out of resources.
3. Updated ME to 11.11.55.1509 for INTEL-SA-00131 Security Advisory to address CVE-2018-3643 and CVE-2018-3644 security issues.
4. Added M.2 slot option ROM control to the BIOS setup menu.
5. Set Descriptor Region of BIOS Region Write Access to "No".
6. Added "SMBIOS Preservation" Enabled/Disabled item for flash recovery.
7. Fixed inability of system to trigger PERR event via ITOS PCIe software injection.
8. Fixed problem of the system loading defaults for password when pressing F3.
9. Fixed failure of HDD when using IPMI raw command to set boot into UEFI.
10. Fixed inability of ME region to flash when FDT is locked.
11. Fixed inability of system to boot to Windows after re-plugging in SATA HDD in UEFI mode.
12. Fixed problem of pressing "Enter" entering Boot Menu (F11) if ADMIN password is set.

1.1a (04/24/2018)

1. Updated CPU microcode to address 'Spectre' variant 2 (CVE 2017-5715) security issue.
2. Updated BIOS version to 1.1a.
3. Added ability of default password to use AMIBCP tool to modify password function.
4. Fixed failure of "Re-try Boot".
5. Fixed failure of the VMD when using "AOC-SLG3-2M2" add-on card.
6. Fixed failure of IPMI force boot function.
7. Fixed problem of system hanging at 0xA2 if SMC HPET item is enabled.
8. Fixed problem of system repeatedly rebooting when NVIDIA 1080p and M.2 devices are plugged in.
9. Fixed inability of system to populate x-AMI language package.

1.1 (12/18/2017)

1. Updated Skylake microcode to 0200003A.
2. Reduced POST time when enabling FfsIntegrityCheck_SUPPORT and FFS_FILE_CHECKSUM_SUPPORT.

3. Updated ME to 11.11.50.1422.
4. Fixed problem of DMI being cleared when SUM LoadDefaultBiosCfg is run.

1.0 (11/7/2017)

1. Updated ME to 11.11.50.1402.
2. Fixed inability of system time to set to build time when clearing CMOS.
3. Updated RSTe legacy/uEFI option ROM version 5.3.0.1052.
4. Added VGA priority selected by slot feature.
5. Modified GPP_H21 & GPP_D5 to GPO low.
6. Added item to control PERR/SERR report.
7. Disabled all of the clock request by GPIO features from ME setting.
8. Fixed inability of AOC-3008L-L8E to enter setup normally.
9. Fixed problem of TPM 1.2 PS index not being Write-Protected so that the content of TPM 1.2 PS index still can be modified after TPM 1.2 is nvLocked.
10. Fixed problem of the boot order having garbage when IPMI tool set is used to system boot into BIOS setup menu.
11. Fixed problem of incorrect BANK LOCATOR of Type 17 appearing.
12. Fixed failure of ChkSmbiosX64.efi check when using SK Hynix DIMM.
13. Fixed inability of VGA priority to change to auto/onboard VGA when incorrect slot is selected.