IPMI Firmware / BIOS Release Notes Form

Supermicro disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade. All products, computer systems, dates, and figures specified are preliminary based on current expectations, and are subject to change without notice. Supermicro and the Supermicro logo are trademarks of Super Micro Computer, Inc. in the U.S. and/or other countries. Copyright © 2018 Super Micro Computer, Inc. All rights reserved.

Product Name	**X11SRM-F/VF**
Release Version	**1.2b**
Release Date	**4/29/2019**
Previous Version	**1.2a**
Update Category	**Critical**
Dependencies	**None**
Important Notes	**None**
Enhancements	**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 for INTEL-SA-00233 Security Advisory to address CVE-2018-12126, CVE-2018-12127 and CVE-2018-12130.
New features	N/A
Fixes	1. Fixed problem of system boot working slowly into PXE. 2. Fixed inability of NMI to trigger BSOD. 3. Fixed the range of BIOS setup menu item VLAN ID from 1 to 4094.

Release Notes from Previous Release(s)

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.*