

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 | X10DRW-E/N(T) |
| Release Version | 3.1 |
| Release Date | 6/7/2018 |
| Previous Version | 3.0a |
| Update Category | Critical |
| Dependencies | None |
| Important Notes | None |
| Enhancements | <ol style="list-style-type: none"> 1. Updated CPU microcode to address 'Spectre' derivatives (CVE-2018-3639 & CVE-2018-3640) security issue. 2. Changed BIOS version to 3.1. 3. Updated Broadwell-EP RC 4.4.0 release. 4. Added support for IPMI IPV6. 5. Removed unsupported memory frequency options from setup menu. |
| New features | N/A |
| Fixes | <ol style="list-style-type: none"> 1. Fixed problem of Afu /O command clearing SMC SMBIOS region (\$SMC). 2. Fixed problem of SUM OOB GetSataInfo always showing "Configuration Type" as "AHCI" when setting "Configure SATA as" to |

| | |
|--|---|
| | <p>"RAID" or "IDE".</p> <p>3. Fixed failure of SMBIOS to change to default even if preserve SMBIOS setup item is set to disabled during recovery.</p> <p>4. Set Descriptor Region of BIOS Region Write Access to "No".</p> |
|--|---|

Release Notes from Previous Release(s) – these will be appended at the bottom of the current release notes in italic and in smaller print

3.0a (04/16/2018)

1. Implemented enhancement to address 'Spectre' variant 2 (CVE 2017-5715) security patch issue.
2. Updated SATA RAID OPRM/EFI driver to RSTe PreOS v4.7.0.1014.
3. Updated Intel Server Platform Services 3.1.3.50 for Grantley Refresh Platforms.
4. Removed support for using Ctrl+home to trigger recovery.
5. Changed BIOS revision to 3.0a.
6. Changed Memory correctable threshold to 100 and enabled Cloaking for Broadwell CPU E5-26xx SKU.
7. Patched workaround for QPI error.

2.0b(07/26/2016)

1. Update Broadwell-EP RC 3.6.0 PLR4 release.
2. Update Haswell-EP C0,1/M0,1/R2 CPU uCode M6F306F2_00000038.
3. Update CPU microcode for Broadwell-EP B0/M0/R0 MEF406F1_0B00001B.
4. Update Intel Server Platform Services 3.1.3 36.0 PLR3 for Grantley Refresh Platforms
5. Add Viking NVDIMM support.
6. Fixed an issue that OS installed under IDE mode failed to boot after BIOS Lock is enabled for security.
7. Add 3 Strike for NVDIMM restore.
8. Add Netlist NVDIMM support.
9. Fixed "VGA Priority" setting malfunctioned when CSM Support item was disabled in BIOS Setup.
10. Fixed SUM InBand flash BIOS in Linux fail when FDT is different.
11. Update SATA RAID OPRM/EFI driver to v4.5.0.1012 (RSTe package 4.5.0.1333).
12. Update TCG2 Label 08
13. Fixed a defect DIMM with very small margin was reported at incorrect location on POST screen and IPMI SEL.
14. Exposed CF9 Global Reset item in BIOS Setup since key customers need this function for NVDIMM.
15. Update Intel Network Software 20.5 PV 10G uEFI driver for new LAN chip supported
16. Fixed healthy DIMMs behind a memory channel where a defect DIMM existed got incorrectly disabled.
17. Synchronized BIOS Build Date with DMI Type 0.
18. Fixed that High Precision Event Timer always shows up in Windows Device Manager when it was set to "Disabled" in setup menu.
19. Enable BIOS and SPI Lock function for security.
20. Clear bit 25 in MSR 0x1FC when HWPM native mode enabled.
21. Add Intel X550 (0x15638086) in SmcDevReport module for reporting it to BMC.
22. Fixed TPM 2.0 issues found during Windows Server 2016 WHQL certification.
23. Modify loop number to match the actual Bank Table list.
24. Fixed Security Device Support item when disabled the Security Device Support, the Security Device Support item will be hidden after reboot.
25. Fix memory freq cannot be set manually when BDW has two 2133 DIMM per channel
26. Set SMBIOS type 39's location field as PSU1, PSU2.
27. Update PXE OPRM to 1.5.72 for i350.
28. To fix boot order sub menu will become abnormal if load setup default before change boot order issue.
29. Update BIOS ACM 3.1.0 PW, SINIT ACM 3.1.0 PW.
30. Enhanced Network boot instance followed BBS priorities.
31. Fixed boot order priority not working properly if change group and sub menu at the time problem.
32. Fixed disable UEFI boot group function fail problem.
33. Fixed USB floppy/key boot instance function not work if multiple mixed USB types devices plugged.
34. Fixed UCE DIMM location could be incorrect at sometimes by MEI.

35. Disabled GPIO_C/D PMSync & C0 Transmit.
36. Fixed When SEL is Full set to "Erase Immediately" but not working.
37. Added IB device report to IPMI.
38. Fixed boot order priority in sub menu group could not working properly if set "Save Changes" and then set "Save Changes and Reset" in setup.
39. Add factory default key for Secure Boot.
40. Default enable ME MCTP function.
41. Revise memory speed if POR is disabled, esp. for 3PDC
42. Re-enable AUTO_HIDE_NVDIMM to NVDIMM setup items if no NVDIMM present
43. Reset BIOS config by IPMI CMOS clear flag.
44. removing warning message when enabled secure boot and patch secure boot support item can be enabled immediately.
45. grayout CSM item when secure boot control item set to enable.
46. patch CTRL+HOME can't work via console
47. [SUM] Fixed "Test_case_320 - Inband - BIOS Config should not change after do change bioscfg and update bios failed.
48. Enable Reset/S5 trigger ADR function
49. Fixed TCG2 event log data is incorrect when loading TE image.
50. Fixed issue ACPI status does not be changed by IPMI when boot to Redhat Server 6.6.
51. Fix no Manufacturer string in SMBIOS type 17 when plugging Kingston DIMM.
52. Fixed WatchDog triggering NMI stress test failed.
53. Change memory frequency from MT/s to MHz for consistency
54. Fixed system will loop in CPU SMM mode after running BMC FW upgrade loop test over 24 hours.
55. Set default system date and time to 2015/01/01 00:00:00 after clearing CMOS.
56. Fix system hang at setup entrance if too many event logs
57. Modify log memory UCE and map out mechanism.
58. Updated legacy VBIOS and GOP to v.1.02.07.
59. Fixed chassis intrusion status in Sensor Readings of IPMI web will be reset after AC on.

2.0a(02/03/2016)

1. Update CTLE value for NVME port with Broadwell CPU.

2.0(12/17/2015)

1. Support AHCI controller M.2(Samsung SM951)
2. Add BMC VLAN items in BIOS setup.
3. To avoid potential issue when BMC no respond in some case.
4. Update Intel Server Platform Services 3.1.3 021.0 PV release for Grantley Refresh Platforms
5. Set PSU characteristic according to FRU
6. Fixed logic error in SmcDevReport module.
7. Moved X710 SSID and SVID to 10G table because quad-port is 10G LAN.
8. Fix UCE cannot be logged
9. Fix recovery issue.
10. Update MPTPM.bin for legacy OS TPM 1.2 problem. (AMI does not add into TCG2_06, binary from EIP237379)
11. Update Broadwell-EP B0/M0/R0 CPU uCode MEF406F1_0B000010.
12. Update Grantley Refresh RC 3.0.0
13. Update TCG2 module to Label TCG2_07.
14. Update Intel Network Software 20.5 LAN Giga and 10G UEFI driver for new LAN chip supported
15. Add sSATA and ISATA string into HDD information in setup menu.
16. Update BIOS ACM 3.0.2 PW.

17. Fix riser card strings show incorrectly in IIO page.
18. Fixed issue that system hangs by writing 0x1 value to 0xB2 port.
19. Fix incorrect BMC firmware revision when minor value less than ten.
20. Fixed Samsung SM951 M.2 can't install OS.
21. Fixed intel XL710 for 40GbE QSPF+ (rev 01) can't show temperature in BMC web.
22. Enable SAMSUNG_3DS_SUPPORT by default.
23. Enable NVMe driver to support Samsung NVMe device.
24. Expose "Home Dir Snoop with IVT- Style OSB" setup item.
25. Fixed issue that memory map out function could not work.
26. Fix smbios type 2 Board Version default value is not "0123456789".
27. Fix DMI lost after clear event log.
28. Fixed issue that cannot pass check OA key test tool.

1.0b(09/16/2015)

- 1.Fixed CPU usage is very high in RHEL 7.0 when switched Hyper-Threading setting.
- 2.Fixed CPU information show at wrong area in TEXT mode.
- 3.Default set SYSTEM_PRODUCT_NAME to "Super Server" per decision.
- 4.Fixed HDD SMART error message show wrong place.
- 5.Fixed runtime UECC error message not show on screen.
- 6.Do not allow can only press "Enter" to enter BIOS SETUP menu if USER password not exist
- 7.Update SPS F/W to SPS_E5_03.00.07.154.0_PLR6-G_WBG_REL.
- 8.To patch LSI 2108 card hang while loading OPRM issue.
- 9.Add workaround to fix Intel 82599(10G) LAN UEFI iSCSI function fail problem.
- 10.Update SATA RAID OPRM/EFI driver to v4.2.0.1036 (RSTe package 4.2.0.1143).
- 11.Update RC 1.14
- 12.Show the CPLD Version in BIOS Setup.
- 13.NV-DIMM support.
- 14.Update Intel SATA & sSATA RAID OPRM and UEFI to 4.3.0.1018.
- 15.Update Microcode "00000036" for C0, C1, M1.
- 16.Update SPS to "3.0.7.173".
- 17.Update Intel RC 1.17.
- 18.Update Intel ACM "20150624".
- 19.Added checksum check and retry for PSU FRU information request from BMC to patch PSU information missing in SMBIOS
- 20.Fixed BMC network related settings in BIOS setup menu not sync with real condition problem.
- 21.Fixed CPU usage is very high in RHEL 7.0 when switched Hyper-Threading setting.
- 22.Don't allow customer enter BIOS setup menu w/o enter password with user competence if only supervisor password set.
- 23.Update AER/MCE related code. Always hide it from setup menu but show message on POST screen.
- 24.Set the sensor scan period of "PIA BMC Platform Power Reading" to 100ms for NM predictive power limit policy feature.
- 25.Show the CPLD Version in BIOS Setup.
- 26.Improve the NVDIMM code and supported Viking NVDIMM.
- 27.Don't hide QPI1 for all 1HA CPU. Only hide QPI1 for EN-2S and EN-UP CPU.
- 28.Set XHCI default disabled in setup menu for old Redhat hang 6.x issue.
- 29.SMBIOS update.
- 30.UEFI LAN driver loading rule changed.
- 31.Support RSC-W-88 riser card.

1.0a(01/07/2015)

1. Updated Intel RC 1.11
2. Updated ME firmware to 3.0.7.154
3. Added the POST Progress Message function support.
4. Implement failure DIMM information to early video screen.
5. To fix cannot log fail DIMM into IPMI on CPU2 problem.
6. Updated Intel TXT ACM modules with BIOS ACM 2.0.
7. Added Intel Haswell-EP supported.- Rev 02D for Intel Haswell-EP C-0, C-1, M-1.

1.0(12/10/2014)

1. First Release.

Product Manager

Date