IPMI Firmware / BIOS Release Notes Form

Product Name	**X10SRi-F**
Release Version	**3.1**
Release Date	**6/6/2018**
Previous Version	**3.0a**
Update Category	**Critical**
Dependencies	**None**
Important Notes	**None**
Enhancements	**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	**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**

	"RAID" or "IDE".
	3. Fixed failure of SMBIOS to change to default even if preserve SMBIOS setup item is set to disabled during recovery.
	4. Fixed problem of the system debug card hanging at 79h after setting JBR1 to pins 2-3 (BIOS RECOVERY).
	5. Set Descriptor Region of BIOS Region Write Access to "No".

3.0a (02/08/2018)

1. Updated Haswell-EP C0,1/M0,1/R2 CPU microcode M6F306F2_0000003C and Broadwell-EP B0/M0/R0 CPU microcode MEF406F1_0B00002A to address 'Spectre' variant 2 (CVE 2017-5715) security issue.

2. Updated SATA RAID OPROM/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 Memory correctable threshold to 100 and enabled Cloaking for Broadwell CPU E5-26xx SKU.

6. Changed BIOS revision to 3.0a.

7. Updated Broadwell-EP RC 4.3.0 PLR10 release.

8. Removed the "P1" string when Memory error occurs on UP server.

9. Corrected POST diagnostic signOn string.

10. Patched Micron Z11C DIMM to improve stability.

11. Changed tCCD_L Relaxation default to 1 and changed string from Enabled to Auto.

12. Appended VPD - VB tag in VPD-W Tag(0x91) area.

13. Updated new MRC error log definition.

14. Added Intel SPI vulnerability patch for Grantley.

15. Added "SMBIOS Preservation" Enabled/Disabled item for flash recovery.

16. Enhanced SMC Recovery Flash Boot Block feature.

17. Displayed setup item "ACS Control" to Enable/Disable PCIe Access Control Services Extended Capability.

18. Added BBS reset function to SmcOobLoadBiosDefault().

19. Added SumBbsSupportFlag into DAT file.

20. Implemented SMC Recovery Flash Boot Block feature.

21. Fixed issue of SUM TC306 and TC317 failing in certain configuration cases.

22. Fixed problem of system resetting or hanging after Watch Dog function is enabled and then BIOS is updated.

23. Fixed incorrect memory error location on UP server.

24. Fixed problem of system hanging on POST code 0xB2.

25. Fixed problem of system resetting or hanging after Watch Dog function is enabled during BIOS update.

26. Fixed inability to get correct Memory CECC DIMM location via SD5.

27. Fixed inability to log Patrol Scrub UCE.

28. Fixed problem of incorrect PCI slot number showing on Legacy/UEFI mode.