BIOS Release Notes Form

Product Name	**X10SRM-(T)F**
Release Version	**3.3**
Release Date	**10/28/2020**
Build Date	**10/28/2020**
Previous Version	**3.2**
Update Category	**Recommended**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Changed BIOS revision to 3.3.** **2. Updated Haswell-EP C0,1/M0,1/R2 CPU microcode version 0x44 for INTEL-SA-00358 Security Advisory to address CVE-2020-0590 (7.7, High), 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. Prevented abnormal display when installing the AMD MI25 and setting the VGA priority to off-board.** **4. Prioritized Disk SMART error event before displaying disk SMART error.** **5. Updated Grantley Refresh RC for INTEL-SA-00390 Security Advisory to address CVE-2020-8764 (8.2, High), CVE-2020-8738 (7.5, High), CVE-2020-8740 (6.7, Medium), and CVE-2020-8739 (4.6, Medium) security issues.**

New features	**N/A**
Fixes	**N/A**

Release Notes from Previous Release(s)

3.2 (11/22/2019)

1. Changed BIOS revision to 3.2.
2. Updated SINIT ACM 3.1.4 PW for INTEL-SA-00240 Security Advisory to address CVE-2019-0151 (7.5, High) and CVE-2019-0152 (8.2, High) security issues.
3. Updated SATA/sSATA RAID OPROM/EFI driver to VROC PreOS v6.2.0.1034.
4. Updated Broadwell-EP B0/M0/R0 CPU microcode MEF406F1_0B000038 for INTEL-SA-00219 Security Advisory to address CVE-2019-0117 (6.0, Medium) security issue and for INTEL-SA-00220 Security Advisory to address CVE-2019-0123 (8.2, High) and CVE-2019-0124 (8.2, High) security issues.
5. Updated AMI EIP453732, EIP470365, EIP451538, and CryptoPkg 32.01 for AMI SA50066.

3.1c (5/3/2019)

1. Changed BIOS revision to 3.1c.
2. Updated Intel Server Platform Services 3.1.3.72 for Grantley Refresh Platforms for INTEL-SA-00213 Security Advisory to address CVE-2019-0089, CVE-2019-0090, CVE-2019-0086, CVE-2019-0091, CVE-2019-0092, CVE-2019-0093, CVE-2019-0094, CVE-2019-0096, CVE-2019-0097, CVE-2019-0098, and CVE-2019-0099 security issues.
3. Updated Haswell-EP/Broadwell-EP CPU microcode from SRV_P_273 for INTEL-SA-00233 Security Advisory to address CVE-2018-12126, CVE-2018-12127, and CVE-2018-12130 security issues.
4. Forced a global reset if SPI descriptor is not write-protected after BIOS flash.
5. Implemented anti-rollback for FDT Read-Only.
6. Implemented multi-line IPMI page text and string.
7. Updated EIP393007 & EIP411789 for TPM vulnerability when resuming S3.
8. Updated SATA/sSATA RAID OPROM/EFI driver to VROC PreOS v6.1.0.1017.
9. Updated VBIOS and VGA EFI Driver to 1.09 to fix ASpeed CVE-2019-6260 security issue.
10. Updated valid range of IPMI setup item VLAN ID to 1-4094.
11. Added support for RFC4122 UUID format feature to set RFC4122 encoding from build time produced by IPMICFG 1.29 tool or newer.
12. Added support for setting IPv6 Static Router1 prefix length and value in BIOS setup menu feature.
13. Fixed problem of BIOS always retrying boot when Re-Try Boot is Disabled.
14. Fixed malfunction of METW if many error events are triggered within a very short time.
15. Displayed the driver health support pages to support LSI (Broadcom 9440-8i) driver health status.
16. Fixed malfunction of Windows Consistent Device Naming (CDN).
17. Fixed the issue of GUID showing zero when using LAN1 for PXE boot on X10SRM-TF.

3.1 (6/8/2018)

1. Updated CPU microcode to address 'Spectre' derivatives (CVE-2018-3639 & CVE-2018-3640) security issue.
2. Changed BIOS version to 3.1.
3. Added support for IPMI IPV6.
4. Removed unsupported memory frequency options from setup menu.
5. Fixed inability of SUM utility to get "Setup Prompt Timeout" setup item.
6. Updated Broadwell-EP RC 4.4.0 release.
7. Fixed problem of Afu /O command clearing SMC SMBIOS region ($SMC).
8. Fixed problem of SUM OOB GetSataInfo always showing "Configuration Type" as "AHCI" when setting "Configure SATA as" to "RAID" or "IDE".
9. Fixed inability to enter setup menu by pressing "DEL" key if Re-try Boot feature is enabled and there are no boot devices.
10. Fixed failure of SMBIOS to change to default even if preserve SMBIOS setup item is set to disabled during recovery.
11. Set Descriptor Region of BIOS Region Write Access to "No".
12. Fixed the issue of UEFI Boot option becoming "Disabled" if HDD is re-plugged in with UEFI Windows on its native installation environment.

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. Changed BIOS revision to 3.0a.
3. Updated SATA RAID OPROM/EFI driver to RSTe PreOS v4.7.0.1014.
4. Updated Intel Server Platform Services 3.1.3.50 for Grantley Refresh Platforms.
5. Removed support for using Ctrl+home to trigger recovery.
6. Changed Memory correctable threshold to 100 and enabled Cloaking for Broadwell CPU E5-26xx SKU.
7. Fixed problem of system not prompting "iKVM doesn't support add-on VGA device. Please change the D-SUB connector to Add-on VGA device..." on POST screen when setting VGA priority to "Offboard".
8. Fixed failure of UEFI OS to boot or install when disabling BMC by motherboard jumper "JPB1" or by setting "BMC Support" to Disabled via BIOS setup.