BIOS Release Notes Form

Product Name	**X10DRi(-T)**
Release Version	**3.4a SPS: 3.1.3.72**
Build Date	**8/16/2021**
Previous Version	**3.4**
Update Category	**Recommended**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Changed BIOS revision to 3.4a.**
New features	**N/A**
Fixes	**1. Fixed failure of OPROM firmware to appear on bootup.**

Release Notes from Previous Release(s)

3.4 (6/14/2021)

1. Changed BIOS revision to 3.4.
2. Updated Intel microcodes 0x46 for Haswell-EP and 0x3E for Broadwell-EP.
3. Updated for IPU 2021.1.

3.3 (3/3/2021)

1. Changed BIOS revision to 3.3.
2. Updated Intel microcode 0x44 for Haswell-EP.
3. Updated Grantley Refresh RC IPU2020.2 to address Intel-TA-00358: CVE-2020-0591 (6.7, Medium) and CVE-2020-0592 (3, Low), and Intel-TA-00390: CVE-2020-8738 (7.5, High), CVE-2020-8740 (6.7, Medium), and CVE-2020-8764 (8.2, High) security issues.

3.2a (5/14/2020)

1. Changed BIOS revision to 3.2a.
2. Updated initial value of memory tccd.
3. Updated outband SMBIOS after tool (inband) update.

3.2 (11/22/2019)

1. Changed BIOS revision to 3.2.
2. Updated Broadwell-EP B0/M0/R0 CPU microcode MEF406F1_0B000038 for Intel-SA00219 (CVE-2019-0117) and Intel-SA00220 (CVE-2019-0123).
3. Updated SINIT ACM 3.1.4 PW for Intel-SA00240 (CVE-2019-0151 CVSS 3.1: 7.5 High).
4. Enabled RFC4122 UUID support.

3.1b (5/16/2019)

1. Changed BIOS revision to 3.1b.
2. Updated Intel microcode 0x43 for Haswell-EP and 0x36 for Broadwell-EP to address Intel-SA-00233 security issue.
3. Updated Intel SPS firmware to E5_03.01.03.072.0_WBG_REL to address Intel-SA-00213 security issue.

3.1a (4/16/2019)

1. Changed BIOS revision to 3.1a.
2. Updated ASPEED VBIOS to version 1.09.00.
3. Updated RSTe SATA/sSATA driver to v6.1.0.1017.

3.1 (9/14/2018)

1. Updated CPU microcode to address 'Spectre' derivatives (CVE-2018-3639 & CVE-2018-3640) security issue.
2. Changed BIOS version to 3.1.
3. Updated Intel RC code to v4.4.0.
4. Removed unsupported memory frequency options from setup menu.
5. Changed the CECC Error Threshold Count to 100.

6. Set Descriptor Region of BIOS Region Write Access to "No".
7. Fixed failure of "Wait for F1 if Error" function to work properly.
8. Fixed problem of power supply PWS-865-PQ FRU information showing incorrectly.

3.0a (2/6/2018)

1. Implemented enhancement to address 'Spectre' variant 2 (CVE 2017-5715) security patch issue.
2. Changed BIOS revision to 3.0a.
3. Updated Intel RC code to v4.3.0.
4. Updated Intel BIOS ACM firmware to v3.1.0 and SINIT ACM firmware to v3.1.1.