IPMI Firmware / BIOS Release Notes Form

Product Name	**X11DDW-L/NT**
Release Version	**3.1 SPS: 4.1.04.296**
Release Date	**04/30/2019**
Previous Version	**3.0c**
Update Category	**Recommended**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Updated Skylake-SP/Cascade Lake-SP CPU microcode.** **2. Updated Intel BKCWW16 2019 PV PLR1.** **3. Updated SPS_E5_04.01.04.296.0 from BKC WW16 2019.** **4. Updated EIP467272 for AMI SA50069, SA50070.** **5. Displayed 3rd IPMI version in BIOS setup.** **6. Set SDDC Plus One or SDDC to disabled by default.** **7. Updated SATA/sSATA RAID OPROM/EFI driver to VROC PreOS v6.1.0.1017.** **8. Optimized setting for SPEC power test.** **9. Changed BIOS revision to 3.1.**
New features	**N/A**
Fixes	**1. Fixed problem of system halting or rebooting at POST code 0xB2 or 0x92 when total GPT partition number is more than 256 and RSD is enabled.** **2. Fixed inability to change IPv6 address or IPv6 Router1 IP address.**

3.0c (3/30/2019)

1. Updated Intel BKCWW10 2019 PV MR3.
2. Enhanced BIOS setup menu to auto-switch the Option ROM's value and hide the unexpected value when boot mode changes.
3. Updated to SPS 4.0.04.381 or above for INTEL-SA-00213 Security Advisory.
4. Set SDDC+1/ADDDC to enabled by default.
5. Changed BIOS revision to 3.0c.
6. Added support for Linux built-in utility efibootmgr.
7. Updated valid range of IPMI setup item VLAN ID to 1-4094.
8. Set NVDIMM ADR timeout to 600μs.
9. Fixed incorrect CPU stepping in BIOS setup.
10. Fixed malfunction of BIOS setup item "PPIN control".
11. Temporarily fixed error for SKX (CLX) 4114 CPU memory training with Micron (18ASF2G72PDZ-2G6E1) RDIMM.
12. Fixed failure to boot into VMware OS when set to Maximum Performance even if Monitor/MWAIT is enabled.
13. Modified UEFI network description to IPv4/IPv6 to follow Industry Standard.
14. Patched problem of system hanging at 0x94 when plugging in Nvidia Tesla T4 card.

3.0a (1/12/2019)

1. Added support for Purley Refresh platform.
2. Set BMC MAC address to UUID for system without onboard LAN1 or with onboard LAN1 disabled.
3. Added support for RFC4122 UUID format feature to set RFC4122 encoding from build time produced by IPMICFG 1.29 tool or newer.
4. Updated CPU microcode SRV_P_264 for Skylake-SP H0/M0/U0 CPUs.
5. Disabled unused SPS ME "CUPS IIO" and "Volumetric Airflow" sensor.
6. Fixed problem of setup item "Quiet Boot" staying enabled after flashing BIOS with "Quiet Boot" disabled.

2.2 (11/01/2018)

1. Changed BIOS version to 2.2.
2. Updated CPU microcode SRV_P_259 for Skylake-SP H0/M0/U0 stepping CPUs.
3. Updated SATA RAID OPROM/EFI driver to RSTe PreOS v5.5.0.1028.
4. Updated SPS 4.0.4.393.
5. Updated BIOS ACM 1.3.9 and SINIT ACM 1.3.6.
6. Enhanced M.2 NVMe error reporting.
7. Fixed issue of setup item "Quiet Boot" staying enabled after flashing BIOS when "Quiet Boot" is disabled.

2.1 (9/14/2018)

1. Updated CPU microcode to address 'Spectre' derivatives (CVE-2018-3639 & CVE-2018-3640) security issue.
2. Changed BIOS version to 2.1.

3. Updated 5.12_PurleyCrb_0ACFD088 for Purley Skylake platform PLR7, BKC 2018 WW20.

4. Updated SPS 4.0.4.381 for INTEL-SA-00131 Security Advisory to address CVE-2018-3643 and CVE-2018-3644 security issues.

5. Updated SATA RAID OPROM/EFI driver to RSTe PreOS v5.4.0.1039.

6. Corrected default setting for Enable SmcBusMasterEn setup item.

7. Added BIOS/ME downgrade check for SPS 4.0.4.340.

8. Added support for UEFI mode PXE boot of F12 hot key Net boot.

9. Added one event log to record that the event log is full.

10. Updated BIOS ACM 1.3.7 and SINIT ACM 1.3.4.

11. Displayed PPR setup item.

12. Removed COM1 information from BIOS Setup.

13. Enabled RSD support.

14. Fixed problem of SUM GetSataInfo showing incorrect "Configuration Type" when setting "Configure sSATA as" to "AHCI" or "RAID" on sSATA controller.

15. Fixed problem of Ctrl + Alt + Del causing system to hang after flashing BIOS.

16. Fixed missing NVDIMM ADR setup item.

17. Fixed problem of system hanging when installing Linux OS after COM1 & COM2 IO/IRQ exchange.

18. Fixed issue with IPMI firmware capability to remove multi asset information.

2.0b (3/7/2018)

1. Implemented enhancement to address 'Spectre' variant 2 (CVE 2017-5715) security patch issue.

2. Changed BIOS revision to 2.0b.

3. Added setup item "SmcBusMasterEn" for enabling Parent bridge of the devices in the gSmcPciForceEnableBusMasterList.

4. Updated Purley RC 151.R03.

5. Displayed setup item "ACS Control" to Enable/Disable PCIe Access Control Services Extended Capability, with Enabled as default.

6. Changed CECC Threshold to 100.

7. Changed RC default setting to upgrade POST Memory correctable error to uncorrectable error and map out the channel.

8. Set enabled JBOF support as default.

9. Disabled CPU2 IIO PCIe root port ACPI hot plug function.

10. Fixed issue with IPMI force boot.

11. Fixed problem of SMC skipping first boot option in UEFI mode when retrying boot.

12. Fixed problem of DMI being cleared when running SUM LoadDefaultBiosCfg.

13. Fixed inability of some CPUs to display correct microcode revision under BIOS setup menu.

14. Fixed problem of system hanging in POST when BIOS is updated in UEFI shell and soft-reset is performed.

2.0 (12/6/2017)

1. Changed BIOS revision to 2.0a.

2. Updated CPU microcode for Skylake-EP H0/B0 stepping CPUs.