BIOS Release Notes Form

Product Name	**X11DDW-L/NT**
Release Version	**3.8b SPS: 4.1.04.901**
Build Date	**01/06/2023**
Previous Version	**3.8a**
Update Category	**Recommended**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Changed BIOS revision to 3.8b.** **2. Updated AMI label 5.14_PurleyCrb_0ACLA058 for RC0626.P01 IPU 2023.1** **a. For INTEL-SA-00717 Security Advisory to address CVE-2022-32231 (7.5, High) / CVE-2022-26343 (8.2, High) security issues.** **3. Updated token RC_VERSION_VALUE setting to 626.P01.** **4. Updated Cascade Lake-SP CPU PV microcode for IPU 2023.1.**
New features	**None**
Fixes	**None**

Release Notes from Previous Release(s)

3.8a (10/28/2022)

1. *Updated AMI label 5.14_PurleyCrb_0ACLA057 for RC0623.D09 2022.3 IPU.*
2. *Updated token RC_VERSION_VALUE setting to 623.D09.*
3. *Updated Intel DCPM UEFI driver to 1.0.0.3536.*
4. *Updated Skylake-SP/Cascade Lake-SP CPU PC microcode for IPU 2022.2.*
5. *Fixed the wrong DIMM location in the event log page.*
6. *Modified the string naming from SMCI to Supermicro.*
7. *Removed "Vendor Keys" in security page.*
8. *Fixed the following:*
9. *Refined SMM buffer validation in mmSmbiosELogInitFuncs.c*
10. *Allocated runtime buffer to trigger ELog SMI in DxeSmmRedirFuncs.c*
11. *Updated BIOS ACM 1.7.54, SINIT ACM 1.7.55 PW for IPU2022.1 to address Intel-TA-00161: CVE-2021-0159 (7.8 High) CVE-2021-33123 (8.2 High) and CVE-2021-33124 (7.5 High).*
12. *Updated VROC SATA/sSATA legacy driver to VROC PreOS v6.3.5.1003 Hot Fix to fix 10TB or higher volume drive issue.*
13. *Enabled IScsi_SUPPORT on Purley generation.*
14. *Modified the allocated buffer from EfiBootServicesData to EfiRuntimeServicesData.*
15. *Disabled MROM1 device.*

3.6 (1/20/2022)

1. *Changed BIOS revision to 3.6.*
2. *Updated SATA/sSATA EFI driver to VROC PreOS v7.7.0.1054.*
3. *Updated AEP uEFI driver to 1.0.0.3531 for IPU2021.2.*
4. *Updated AMI label 5.14_PurleyCrb_0ACLA054 for RC0616.D08 2021.2 IPU.*
5. *Updated Intel Server Platform Services to Purley Refresh Server Platforms IPU2021.2 HF1 4.1.4.654.*
6. *Updated BIOS ACM 1.7.51, SINIT ACM 1.7.51 PW.*
7. *Updated Skylake-SP/Cascade Lake-SP CPU PV microcode.*

3.5 (5/27/2021)

1. Updated RC 612.D02 and IPU 2021.1 PV for INTEL-SA-00463 Security Advisory to address CVE-2020-12357 (7.5, High), CVE-2020-8670 (7.5, High), CVE-2020-8700 (7.5, High), CVE-2020-12359 (7.1, High), CVE-2020-12358 (6.7, Medium), CVE-2020-12360 (5.6, Medium), CVE-2020-24486 (5.5, Medium), and CVE-2020-0589 (3.8, Low) security issues.
2. Updated BIOS ACM 1.7.43 and SINIT ACM 1.7.4A PW for INTEL-SA-00463 Security Advisory to address CVE-2020-12357 (7.5, High), CVE-2020-8670 (7.5, High), CVE-2020-8700 (7.5, High), CVE-2020-12359 (7.1, High), CVE-2020-12358 (6.7, Medium), CVE-2020-12360 (5.6, Medium), CVE-2020-24486 (5.5, Medium), and CVE-2020-0589 (3.8, Low) security issues.
3. Updated Skylake-SP/Cascade Lake-SP CPU PV microcode for INTEL-SA-00464 Security Advisory to address CVE-2020-24511 (5.6, Medium) and CVE-2020-24512 (2.8, Low) security issues.
4. Updated Intel Server Platform Services for Purley Refresh Server Platforms 4.1.4.505.
5. Updated AEP firmware to FW_1.2.0.5446 and UEFI driver to 3515 for IPU2021.1.
6. Synced IPv6 status detection rule with BMC to make sure IPv6 status is the same in BIOS and BMC web.

3.4a (1/30/2021)

1. Updated BIOS revision to 3.4a.
2. Fixed inability of system to boot into PXE with DVD installed.

3.4 (11/7/2020)

1. Updated 5.14_PurleyCrb_0ACLA052 for RC update and 2020.2 IPU PV to address Intel-TA-00358: CVE-2020-0587 (6.7, Medium), CVE-2020-0591 (6.7, Medium), CVE-2020-0592 (3, Low), and Intel-TA-00390: CVE-2020-0593 (4.7, Medium), CVE-2020-8738 (7.5, High), CVE-2020-8739 (4.6, Medium), CVE-2020-8740 (6.7, Medium), and CVE-2020-8764 (8.7 High) security issues.
2. Updated BIOS ACM 1.7.41 and SINIT ACM 1.7.49 PW for IPU2020.2 to address Intel-TA-00358: CVE-2020-0588 (3.8, Low) and CVE-2020-0590. (7.7, High) security issues.
3. Updated SPS 4.1.4.423 to address Intel-TA-00391: CVE-2020-8755 (4.6, Medium) and CVE-2020-8705 (7.1, High) security issues.
4. Updated Skylake-SP/Cascade Lake-SP CPU PV microcode from 20200918_NDA Release to address Intel-TA-00381: CVE-2020-8696 (2.5, Low) security issue, MD_Clear Errata, MOB Speedpath, and IRR Restore with RS Throttle (ITR #2).
5. Updated SATA/sSATA RAID OPROM/EFI driver to VROC PreOS v6.3.0.1005 PV.
6. Enhanced SMCI HDD Security feature.
7. Added force next boot to UEFI Shell via IPMI support.
8. Added function to move all LANs to the top of boot priority when IPMI forces PXE.
9. Added inband flash status event log to IPMI MEL.
10. Corrected "Station MAC Address" display order when "Configuration Address Source" is set to "Static".
11. Added PPR success result SEL and set duplicated PPR SELs to be filtered out if the location is same.
12. Added VMWare PMem for VMWware Certification Allowance for PMEM Optane Memory, displayed Config TDP control item, and added help string for HttpBoot item "Input the description".
13. Enabled support for feature for IPMI UEFI PXE booting to all LAN ports.
14. Updated AMI EIP563137 to fix failure of some BIOS items (like boot mode item) to load default with some configurations (like with Micron M.2 or HGST SATA M.2).
15. Fixed problem of EFI version of PassMark MemTest86 hanging when SMCI Redfish Host Interface is not supported in IPMI firmware.
16. Fixed failure of "UEFI Compliant - Boot from iSCSI peripheral" in UEFI SCT test.
17. Fixed problem of system hanging during BIOS flash if Watch Dog function is enabled.
18. Fixed inability of 6240R and some refresh 4 serial CPU frequencies to reach maximum when enabling Mwait.
19. Corrected BMC firmware revision in BIOS Setup.
20. Fixed problem of system hanging at 0xB2 with some NVMe devices.
21. Fixed problem of system hanging at POST code 0xA0 or 0xA2 when using unsupported security NVMe device and installing Hyper-V with Windows 2019.
22. Fixed inconsistency of X-AMI ID of Setup Item "Refresh Watermarks".

3.3 (02/21/2020)

1. Updated BIOS ACM 1.7.40 and SINIT ACM 1.7.48 PW.
2. Added support for SMCI USB Remote Network Driver Interface and SMCI USB Universal Network Device Interface, and for Redfish module to get Processor, Memory, and PCIe information.
3. Added sighting CLX28 workaround and downgraded patrol scrub UC to CE.
4. Added SMC HDD Security feature.

5. Updated Skylake-SP/Cascade Lake-SP CPU microcode for Intel-SA-00329 (CVE2020-0548 2.8 Low and CVE2020-0549 6.5 Medium), Intel-SA-00288 (CVE2019-11157 5.3 Medium), and Intel-SA-00317 (CVE2019-14607 7.9 High).
6. Enhanced PPR log function.
7. Updated AMI label 5.14_PurleyCrb_0ACLA050 beta for IPU2020.1 PV.
8. Updated SPS_E5_04.01.04.381 from IPU 2020.1.
9. Updated setup menu to remove our own tRFC optimization item, add Intel "tRFC Optimization for 16Gb Based DIMM" and "Panic and High Watermark" items, and add "Balanced Profile" option for "DCPMM Performance Setting".
10. Disabled VRM dynamic phase shedding on CPU0/1, DIMM channel A/B/C/D/E/F/G/H.
11. Changed BIOS revision to 3.3.
12. Fixed Intel Self test 7 v111 SPI/DCh BIOS_CNTL to set BIOS Control Register BIT[9] to 1.
13. Fixed inability to log UPI correctable error.
14. Fixed inability to create HTTP/HTTPS boot option when USB UNDI module is enabled.

3.2 (10/16/2019)

1. Updated AMI label 5.14_PurleyCrb_0ACLA049_BETA for BKC WW36 RC595.D04 for AMI security update SA50072, IPU 2019.2 INTEL-SA-00280 Security Advisory to address CVE-2019-11136 (7.5, High) and CVE-2019-11137 (7.5, High) security issues.
2. Updated SINIT ACM 1.7.3 PW from BKC WW36 IPU 2019.2 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 SPS_E5_04.01.04.339.0 from BKC WW36 IPU 2019 for INTEL-SA-00241 Security Advisory to address CVE-2019-11090 (6.8, Medium), CVE-2019-11088 (7.5, High), CVE-2019-0165 (4.4, Medium), CVE-2019-0166 (5.9, Medium), CVE-2019-0168 (4.6, Medium), CVE-2019-0169 (9.6, Critical), CVE-2019-11086 (3.5, Low), CVE-2019-11087 (6.4, Medium), CVE-2019-11101 (4.4, Medium), CVE-2019-11100 (6.1, Medium), CVE-2019-11102 (4.1, Medium), CVE-2019-11103 (7.3, High), CVE-2019-11104 (7.3, High), CVE-2019-11105 (7.9, High), CVE-2019-11106 (4.4, Medium), CVE-2019-11107 (5.3, Medium), CVE-2019-11108 (2.3, Low), CVE-2019-11110 (4.1, Medium), CVE-2019-11097 (7.3, High), CVE-2019-0131 (7.1, High), CVE-2019-11109 (4.4, Medium), CVE-2019-11131 (7.5, High), CVE-2019-11132 (8.4, High), and CVE-2019-11147 (8.2, High) security issues.
4. Updated Skylake-SP/Cascade Lake-SP CPU microcode from Intel-Generic-Microcode-20191004_NDA for INTEL-SA-00271 Security Advisory to address CVE-2019-11139 (5.8, Medium) security issue.
5. Updated SATA/sSATA RAID OPROM/EFI driver to VROC PreOS v6.2.0.1034.
6. Updated VBIOS and VGA EFI Driver to 1.10.
7. Added setup item to control 16Gb based Single Die Package DIMM tRFC optimization.
8. Added recommended AEP DIMM firmware version.
9. Displayed Setup item "ARI Support".
10. Added support for firmware version information.
11. Added support for IPMI 3rd revision.
12. Disabled ADDDC/SDDC and set PPR as hPPR.
13. Changed BIOS revision to 3.2.
14. Added Enhanced PPR function.
15. Masked AP Mwait instruction if needed.

3.1 (04/30/2019)

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.
10. 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.
11. 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.

_____ _____

Product Manager *Date*