# IPMI Firmware / BIOS Release Notes Form



| | |
|---|---|
| **Product Name** | **X11DPL-i** |
| **Release Version** | **3.5** |
| **Release Date** | **5/24/2021** |
| **Previous Version** | **3.4** |
| **Update Category** | **Critical** |
| **Dependencies** | **N/A** |
| **Important Notes** | |
| **Enhancements** | **1. Update RC 612.D02 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.**<br>**2. [Enhancements] Update BIOS ACM 1.7.43, 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.**<br>**3. [Enhancements] 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.**<br>**4. [Enhancements] Updated Intel Server Platform Services for Purley Refresh Server Platforms 4.1.4.505.**<br>**5. [Enhancements] Support IPMI UEFI PXE boot to all LAN port feature.**<br>**6. [Enhancements] Sync IPv6 status detection rule with BMC to make sure IPv6 status is the same in BIOS and BMC web.** |

| | |
|---|---|
| | **7. [Enhancements] Update SATA/sSATA EFI driver to VROC PreOS v7.5.0.1152.**<br>**8. [Enhancements] This system cannot boot into PXE with DVD installed.**<br>**9. [Enhancements] Updated Intel Server Platform Services for Purley Refresh Server Platforms HF 4 PLR 4.1.4.450**<br>**10. [Enhancements] Support IPv6 HTTP Boot function.**<br>**11. [Enhancements] Correct typo in "PCIe PLL SSC" setup item help string.**<br>**12. [Enhancements] Update AEP FW to FW_1.2.0.5446, uEFI driver to 3515 for IPU2021.1.**<br>**13. [Enhancements] Remove intel lan memory 4G limit if boot mode is not legacy.** |
| **New features** | **N/A** |
| **Fixes** | **1. [Fixes] Fix "Configuration Address Source" always show "DHCP" in IPMI IPv6 page.**<br>**2. [Fixes] Fixed UEFI OS boot option name shows incorrectly in BIOS setup.** |

***Release Notes from Previous Release(s)***

***3.4 (3/11/2020)***

1. *Change BIOS version to 3.4*
2. *Updated Skylake-SP/Cascade Lake-SP CPU PV microcode from 20200918_NDA Release to address Intel-TA-00381: CVE-2020-8696 (2.5 Low) and MD_Clear Errata, MOB Speedpath and IRR Restore with RS Throttle (ITR #2).*
3. *Update 5.14_PurleyCrb_0ACLA052_BETA for RC update and 2020.2 IPU PV to addresses Intel-TA-00358: CVE-2020-0587 (6.7 Medium), CVE-2020-0591 (6.7 Medium), CVE-2020-0592 (3 Low),*
   *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), CVE-2020-8764 (8.7 High); INTEL-TA-00391: CVE-2020-8752(9.4, Critical), CVE-2020-8753(8.2, Critical), CVE-2020-12297(8.2, Critical), CVE-2020-8745(7.3, Critical), CVE-2020-8705(7.1, Critical), CVE-2020-12303(7.0, Critical), CVE-2020-8757(6.3, Medium), CVE-2020-8756(6.3, Medium), CVE-2020-8760(6.0, Medium), CVE-2020-8754(5.3, Medium), CVE-2020-8747(4.8, Medium), CVE-2020-12356(4.4, Medium), CVE-2020-8746(4.3, Medium), CVE-2020-8749(4.2, Medium). INTEL-SA-00358: 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), CVE-2020-0592(3.0, Low). INTEL-TA-00391: CVE-2020-8744(7.2, High), CVE-2020-8705(7.1, High), CVE-2020-8755(4.6, Medium). AMI SA50080 and AMI SA50081: CVE-2020-0570(7.6, High), CVE-2020-0571(5.5, Medium) and CVE-2020-8675(7.1, High). AMI SA-50085: CVE-2020-10713 (8.2, High), AMI SA-50084: CVE-2020-10255 (9, High)*
4. *Updated SPS 4.1.4.423 to address Intel-TA-00391: CVE-2020-8755 (4.6 Medium) CVE-2020-8705 (7.1 High)*
5. *Update BIOS ACM 1.7.41, SINIT ACM 1.7.49 PW to addresses Intel-TA-00358: CVE-2020-0588 (3.8 Low) and CVE-2020-0590. (7.7 High)*
6. *Update SATA/sSATA RAID OPROM/EFI driver to VROC PreOS v6.3.0.1005 PV*
7. *Update AEP FW to FW_1.2.0.5444 to match IPU2020.2.*
8. *Enable token "IPMI_FORCE_BOOT_UEFI_SHELL" to support to shell by ipmi change boot order command.*
9. *Move all LANs to the top of boot priority when IPMI force PXE.*
10. *Add inband flash status event log to IPMI MEL.*
11. *[ALL] enhancement - "Redfish Managers.Network Protocol" SSDP catalog*
12. *[ENGINEERING] Default disable SSDP*
13. *[ENGINEERING] enhancement - block more invalid input for Configuration Web*
14. *[ENGINEERING] enhancement - Visa Security Sensitive parameters improvme*
15. *AOC NIC Temp sensor reading shows n/a*
16. *Invalid NVMe Temp critical warning SELs when hot inserted NVMe*
17. *[ENGINEERING] enhance - Sync SW team SELs severity and description*

***3.3 (21/2/2020)***

1. *Changed BIOS version to 3.3.*
2. *Updated Skylake-SP/Cascade Lake-SP CPU microcode for Intel-SA-00329 (CVE2020-0548 2.8 Low, CVE2020-0549 6.5 Medium), Intel-SA-00288 (CVE2019-11157 5.3 Medium), Intel-SA-00317 (CVE2019-14607 7.9 High)*
3. *Updated AMI label 5.14_PurleyCrb_0ACLA050 beta for IPU2020.1 PV.*
4. *Updated SPS_E5_04.01.04.381 from IPU 2020.1 PV*
5. *Updated BIOS ACM 1.7.40, SINIT ACM 1.7.48 PW*
6. *Patched system hang at 94 with NVIDIA new RTX 6000/8000*
7. *Saved memory ce location into PPR variable at runtime even if memory correctable error reporting is disabled.*

8. *Added setup item "HDD password prompt Control" to control "Hard-Drive Password Check" enable/disable HDD password prompt window during POST.*
9. *Added SMC HDD Security feature.*
10. *Added RedFish functions Support*
11. *Fixed system keep reset under ATTO Fiber network card legacy OPROM user menu issue.*
12. *Fixed Secure Boot Mode value mismatch.*
13. *Fixed there is no need to use Admin password for erasing TCG device.*
14. *[Fixes] Fix two CentOS boot items in boot order if CentOS installed in RAID 1 system.*

***3.2 (12/2/2019)***

1. *Changed BIOS version to 3.2.*
2. *Updated AMI label 5.14_PurleyCrb_0ACLA049_BETA for BKC WW36 IPU 2019.2 and AMI security update SA50072.*
3. *Updated SINIT/BIOS ACM from BKC WW36 IPU 2019.2 address CVE-2019-0151 and CVE-2019-0152.*
4. *Updated SPS_E5_04.01.04.339.0 from BKC WW36 IPU 2019.2 adress PSIRT-TA-201905-011.*
5. *Updated Cascade Lake-SP CPU microcode and Skylake-SP microcode.*
6. *Updated Cascade Lake-SP A0 stepping CPU microcode.*
7. *Updated SATA/sSATA RAID OPROM/EFI driver to VROC PreOS v6.2.0.1034 PC.*
8. *Exposed Setup item "ARI Support".*
9. *Updated 16Gb based Single Die Package DIMM tRFC optimization to control by setup.*
10. *Updated Secure Boot Key for fixing the error message of PK key.*
11. *Added back erase NVDIMM routine.*
12. *Updated VBIOS and Vga EFI Driver to 1.10.*
13. *Enhanced F12 hot key PXE boot feature.*
14. *Updated the behavior for the feature that update SMBIOS Type 1 and 3 with Fru0.*
15. *Added Redfish/SUM Secure Boot feature, update OOB for secure boot and reserve Key.*
16. *Disabled ADDDC/SDDC and set PPR as hPPR by Intel's suggestion for memory error.*
17. *Added sighting CLX28 workaround, downgrade patrol scrub UC to CE.*

***3.1 (5/21/2019)***

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. *Set SDDC Plus One or SDDC as Disabled by default.*
6. *Updated SATA/sSATA RAID OPROM/EFI driver to VROC PreOS v6.1.0.1017.*
7. *Set Leakey bucket to decrease one memory correctable error count within 2.15 minutes and threshold 512.*
8. *Set ADDDC Sparing to enable by default.*
9. *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.*

***3.0b (3/4/2019)***

1. *Added support for Purley Refresh platform.*

2. *Updated SPS to 4.1.04.256 (4.1.02.174 or above) for INTEL-SA-00185 Security Advisory RC to 576.D20 (549.D13 or above) for INTEL-SA-00192 Security Advisory.*
3. *Updated CPU microcode for Skylake-SP H0/M0/U0 stepping CPUs.*
4. *Added support for Monitor Mwait feature.*
5. *Set BMC MAC Address to UUID for system without onboard LAN1 or with onboard LAN1 disabled.*
6. *Updated SATA RAID OPROM/EFI driver to RSTe PreOS v6.0.0.1024.*
7. *Set PCIe correctable and uncorrectable (non-fatal) error report to disabled by default.*
8. *Added support for RFC4122 UUID format feature to set RFC4122 encoding from build time produced by IPMICFG 1.29 tool or newer.*
9. *Updated CPU microcode SRV_P_262 for Skylake-SP H0/M0/U0 CPUs.*
10. *Disabled unused SPS ME "CUPS IIO" and "Volumetric Airflow" sensor.*
11. *Added 2933 to memory POR.*
12. *Added support for Linux built-in utility efibootmgr.*
13. *Updated valid range of IPMI setup item VLAN ID to 1-4094.*
14. *Added driver health warning message.*
15. *Set NVDIMM ADR timeout to 600us..*
16. *Fixed malfunction of CPU PBF (Prioritized Base Frequency).*
17. *Fixed problem of setup item "Quiet Boot" staying enabled after flashing BIOS with "Quiet Boot" disabled.*
18. *Fixed incorrect PBF high frequency core number when Hyper-Threading is disabled.*
19. *Added workaround for failure of BIOS flash with 156 bytes PubKey (Error: "Secure Flash Rom Verify Fail").*
20. *Modified UEFI network description to IPv4/IPv6 to follow Industry Standard.*
21. *Patched problem of system hanging at 0x94 when plugging in Nvidia Tesla T4 card.*

***2.1 (6/15/2018)***

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 Purley RC 154.R13, SPS 4.0.04.340 and ACM 1.3.7, SINIT ACM 1.3.4.*
4. *Updated SATA RAID OPROM/EFI driver to RSTe PreOS v5.4.0.1039.*
5. *Added BIOS/ME downgrade check for SPS 4.0.4.340.*
6. *Added support for UEFI mode PXE boot of F12 hot key Net boot.*
7. *Added one event log to record that the event log is full.*
8. *Displayed PPR setup item.*
9. *Added support for SATA FLR.*
10. *Fixed problem of SUM GetSataInfo showing incorrect "Configuration Type" when setting "Configure sSATA as" to "AHCI" or "RAID" on sSATA controller.*
11. *Fixed problem of Ctrl + Alt + Del causing system to hang after flashing BIOS.*
12. *Fixed problem of system hanging when installing Linux OS after COM1 & COM2 IO/IRQ exchange.*
13. *Rolled back SVN_3413 to fix failure of WDT function*.

***2.0b (3/6/2018)***

1. *Updated CPU microcode SRV_B_216 for Skylake-SP H0/M0/U0 stepping CPUs to address 'Spectre' variant 2 (CVE 2017-5715) security issue.*
2. *Changed BIOS version to 2.0b.*
3. *Updated 5.12_PurleyCrb_0ACFD085Beta for Purley Skylake platform PLR 4, BKC WW02.*
4. *Displayed setup item "ACS Control" to Enable/Disable PCIe Access Control Services Extended Capability, with Enabled as default.*
5. *Updated BIOS ACM 1.3.5 and SINIT ACM 1.3.3.*

6. *Disabled CPU2 IIO PCIe root port ACPI hot plug function.*
7. *Fixed IPMI force boot issue.*
8. *Fixed malfunction of "SMBIOS Preservation" Disabled.*
9. *Fixed problem of SMC skipping first boot option in UEFI mode when retrying boot.*
10. *Fixed inability to reset the system under DOS by pressing "Ctrl-Alt-Del" on USB keyboard when "Port 60/64 Emulation" is disabled.*
11. *Fixed inability of some CPUs to display correct microcode revision under BIOS setup menu.*
12. *Hid unused items "Onboard NVME1\2 Option ROM" in BIOS setup menu.*
13. *Fixed inability of IPMI Web to report correct information for customer PSU "GW-ERP1U450-2H".*

***2.0 (11/29/2017)***

1. *Changed BIOS revision to 2.0.*
2. *Updated SATA RAID OPROM/EFI driver to RSTe PreOS v5.3.0.1052.*
3. *Updated BIOS ACM 1.3.4.*
4. *Updated SPS to 4.0.4.294.*
5. *Updated CPU microcode SRV_P_214 for Skylake-EP H0/M0/U0 stepping CPUs.*
6. *Updated 5.12_PurleyCrb_0ACFD084_BETA for Purley Skylake platform PLR 3.1*
7. *Fixed problem of SNC being disabled once NVDIMM is present in system.*
8. *Fixed problem of DMI being cleared when SUM LoadDefaultBiosCfg is run.*