BIOS Release Notes Form

Product Name	**X12QCH+-P (1.01)**
Release Version	**1.8 SPS: 4.4.4.603**
Release Date	**12/22/2023**
Build Date	**12/22/2023**
Previous Version	**1.7**
Updated Category	**Recommended**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Updated the BIOS version to 1.8.** **2. Updated the Cooper Lake A1 stepping CPU microcode MBF5065B_07002802 for IPU 2024.1.** **3. Updated SPS version 4.4.4.603 for INTEL-SA-00923 Security Advisory to address the CVE-2023-35191 (6.8 Medium) security issue.** **4. Updated Intel BKC 2024.1 IPU.** **5. Fixed the lack of a Rocky Linux boot option.** **6. Updated CryptoPkg for AMI SA50193 to address the CVE-2023-0464 (7.5, High) security issue.** **7. Updated CryptoPkg for AMI SA50191 to address the CVE-2023-0465 (5.3, Medium) security issue.** **8. Updated HardwareSignatureManagement for AMI SA50202 to address the CVE-2023-34470 (3.1, Low) security issue.**

	9. **Updated Usb for AMI SA50199.** 10. **Updated TCG2 for AMI SA50198 to address CVE-2022-36763 (6.5, Medium) and CVE-2022-36764 (6.5, Medium) security issues.** 11. **Updated NVRAM for AMI SA50181.** 12. **Updated Keys for AMI SA50182 to address the CVE-2023-28005 (6.8, Medium) security issue.** 13. **Updated Keys for AMI SA50197 to address the CVE-2022-21894 (4.4, Medium) security issue.** 14. **Added PCIe resizable bar function support.** 15. **To expose MCTP per PCIE port.** 16. **Updated the setup template.** 17. **Updated SA50216_Supplement(LogoFAIL Vulnerability).**
New features	**None**
Fixes	**None**

Release Notes from Previous Release(s)

1.7 (10/06/2023)

1. *Updated the BIOS version to 1.7.*
2. *Updated Cooper Lake A1 stepping CPU microcode MBF5065B_07002703 for INTEL-TA-00828 Security Advisory to address CVE-2022-40982(6.5, Medium) security issue.*
3. *Updated SPS version 4.4.4.500 for IPU 2023.3.*
4. *Updated Intel BKC 2023.3 IPU for INTEL-TA-00813 Security Advisory to address CVE-2022-43505(4.1, Medium) security issue.*
5. *Updated VROC sSATA/SATA driver version 8.0.0.4006.*
6. *Updated ASPEED 2500 VBIOS and EFI driver to 1.11.03.*
7. *Default enabled Intel(R) VT for Directed I/O (VT-d).*
8. *Updated the BIOS version to 1.6.*
9. *Updated Cooper Lake A1 stepping CPU microcode MBF5065B_07002601 for IPU 2023.2.*
10. *Updated MdeModulePkg for AMI SA50170 to address CVE-2021-38578 (9.8, High) security issue.*
11. *Supported the system configuration G & H.*
12. *Updated Temperature Offset per system PM request.*
13. *Fixed ENERGY_PERF_BIAS_CFG Mode item change to default after SUM update BIOS with --preserve_setting command.*

1.5 (1/4/2023)

1. *Updated the BIOS version to 1.5.*
2. *Updated Cooper Lake A1 stepping CPU microcode MBF5065B_07002503 for IPU 2023.1.*
3. *Updated SPS version 4.4.4.301 for INTEL-TA-00718 Security Advisory to address CVE-2022-36348 (8.8, High) security issue.*
4. *Updated Intel BKC 2023.1 IPU for INTEL-SA-00717 to address CVE-2022-30539 (7.5, High), CVE-2022-32231 (7.5, High), and CVE-2022-26837 (7.5, High) security issues.*
5. *Updated VROC sSATA/SATA driver version 7.8.0.1012.*
6. *Updated EfiOsBootOptionNames_20 for AMI SA50157 Security Advisory.*
7. *Updated Temperature Offset per system PM request.*

1.3 (7/18/2022)

1. *Updated the BIOS version to 1.3.*
2. *Updated Intel BKC 2022.2 IPU for INTEL-TA-00686 Security Advisory to address CVE-2021-33060 (7.8, High) security issue.*
3. *Updated PMem UEFI version 2.0.0.3886.*
4. *Updated TcgStorageSecurity for AMI SA50110.*
5. *Updated SmmCoreAmiBufferValidationLib for AMI SA50111.*
6. *Updated AmiNetworkPkg for AMI SA50110.*
7. *Updated SmiVariable for AMI SA50116.*
8. *Supported the system configuration D.*
9. *Supported the system configuration E.*
10. *Updated slot id as requested by the system PMs.*

11. Fixed that it couldn't detect m.2 NVMe for system configuration F & G.

11.1 (01/06/2022)

1. *Updated the BIOS version to 1.1.*
2. *Updated Cooper Lake A1 stepping CPU microcode MBF5065B_07002402 for INTEL-SA-00532 Security Advisory to address CVE-2021-0127(5.6, Medium).*
3. *Updated SPS version 4.4.4.048.*
4. *Checked SPS functions like Node management.*
5. *Updated Intel BKC 2021.2 IPU for INTEL-SA-00562 Security Advisory to address CVE-2021-0158(8.2, High).*
6. *Updated BIOSACM version 1.3.2 and SINITACM version 1.3.2 for INTEL-TA-00527 Security Advisory to address CVE-2021-0099(7.8, High), CVE-2021-0107(7.2, High), CVE-2021-0111(7.2, High), CVE-2021-0114(8.2, High), CVE-2021-0115(8.2, High), CVE-2021-0116(8.2, High), CVE-2021-0117(8.2, High), CVE-2021-0118(8.2, High), CVE-2021-0125(6.7, Medium), CVE-2021-0124(6.3, Medium).*
7. *Updated VROC sSATA/SATA driver version 7.6.0.1012.*
8. *Updated PMem UEFI version 2.0.0.3878.*
9. *Added flag [Preserve BIOS Boot Options Configuration] controlled by BMC/SUM.*
10. *Redefined Enhanced PPR for AMT2.0 update.*
11. *Changed string "VMX" to "Intel Virtualization Technology".*
12. *Added support for system configuration F & G.*
13. *Removed 1G option from MMCFG base to avoid system hang.*
14. *Fixed the SMBIOS event log ERROR CODE that is not displaying correctly under BIOS menu issue (EFI error type).*
15. *Fixed the setup item "Lockdown Mode", which is always grayed-out.*
16. *Fixed SpeedStep (P-States) which changes settings when its default setting is set to Disable and load BIOS defaults in Setup.*

1.0c (12/01/2021)

1. *Updated BIOS to version 1.0c.*
2. *Updated SPS version 4.4.4.035.*
3. *Updated 5.19_CedarIslandCrb_0ACMT_016 Intel BKC WW20 PLR2.*
4. *Updated BIOSACM version 1.0.A and SINITACM version 1.0.A.*
5. *Updated VROC sSATA/SATA driver version 7.5.0.1152.*
6. *Updated PMem UEFI version 2.0.0.3866 and PMem FW version 2.2.0.1553.*
7. *Added code to stop AFU support.*
8. *Enhanced Smc Dcpmm feature.*
9. *Extended DIMM memory serial number information. (Samsung, Micron, Hynix)*
10. *Removed Intel LAN memory 4G limit if boot mode is not legacy.*
11. *Set all OPROM control items to Legacy when boot mode set to Dual.*
12. *Set PCH PCI-E ASPM to disabled if CPU PCI-E global ASPM is disabled.*
13. *Updated CPLD Signature table 101.*
14. *Changed "SMCI PMem Formset" to "SMCI PMem Configuration".*
15. *Changed "Hard Drive Security Frozen" default setting to disabled.*

16. Added support for recovering boot status after flashing ROM through BMC/CPLD.
17. Added support for Supermicro Update Manager (SUM) upload/delete HTTPS TLS certificate.
18. Changed BIOS to prevent "Power Performance Tuning" being selected, when loading the BIOS default.
19. Now supports EUI-48 Locally Administered MAC Address.
20. Updated SmcOOB module to 1.01.24 to support SUM clean SMBIOS Event log through BiosCfg header flag.
21. Disabled EFI iSCSI support.
22. Revised Me version strings, removed the "Manufacturer ID" string.
23. Fixed the HDD security menu, it will not show when connecting more than 6 HDDs on the system.
24. Fixed an issue where the IPV6 address still appears even if IPV6 is disabled in the IPMI GUI.
25. Fixed system freeze with Micron 2300 256GB NVMe installed.
26. Fixed an issue where the memory device in IPMI does not match the BIOS setup when some memory DIMMs are mapped out.
27. Fixed UEFI OS boot option name that shows incorrectly in BIOS setup.
28. Fixed to prevent erasure a TCG device without an installed password. Fixed wrong FW version and vendor name in Trusted computing page.
29. Updated SMCOOB to keep the NVRAM variables that should be kept (SGX vars, KMS Vars, ...) when executing "sum.exe -c LoadDefaultBiosCfg".

_____ _____

Product Manager *Date*