# BIOS Release Notes Form



| | |
|---|---|
| **Product Name** | **X12QCH+-P (1.01)** |
| **Release Version** | **1.3** |
| **Release Date** | **07/18/2022** |
| **Build Date** | **07/18/2022** |
| **Previous Version** | **1.1** |
| **Updated Category** | **Recommended** |
| **Dependencies** | **None** |
| **Important Notes** | **None** |
| **Enhancements** | **1. Updated the BIOS version to 1.3.**<br>**2. Updated Intel BKC 2022.2 IPU for INTEL-TA-00686 Security Advisory to address CVE-2021-33060 (7.8, High) security issue.**<br>**3. Updated PMem UEFI version 2.0.0.3886.**<br>**4. Updated TcgStorageSecurity for AMI SA50110.**<br>**5. Updated SmmCoreAmiBufferValidationLib for AMI SA50111.**<br>**6. Updated AmiNetworkPkg for AMI SA50110.**<br>**7. Updated SmiVariable for AMI SA50116.**<br>**8. Supported the system configuration D.**<br>**9. Supported the system configuration E.**<br>**10. Updated slot id as requested by the system PMs.** |

| | |
|---|---|
| **New features** | **None** |
| **Fixes** | **1. Fixed that it couldn’t detect m.2 NVMe for system configuration F & G.** |

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

***1.1 (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*