BIOS Update Release Notes

PRODUCTS:KC71F, KC71E, KC51E

BIOS Version 0048 - KCTGL357.0048.2024.0326.1744

About This Release:

- Date: Mar 26, 2024
- ROM Image Checksum: 0XAA9063C8
- EC Firmware: 1.15.09.000
- ME Firmware: 15.0.47.2473
- PCH Configuration Firmware: 15.0.0.1021
- PMC Firmware: 150.2.10.1020
- iTBT Firmware: 15.0.0.0311
- IOM Firmware: 24.31.0.0000
- Retimer Firmware in BIOS capsule: 2.22
- NPHY Firmware: 15.107.135.5018
- CRB Label: 1AWHY_048
- Boot Guard ACM: 1.14.46
- BIOS Guard: BiosGuard_029
- Silicon Initialization Code: 0A.00.5D.32(4303.02)
- Memory Reference Code: 2.0.2.8
- Integrated Graphics:
    - UEFI Driver: 17.0.1070
- Intel RST Pre-OS:
    - VMD Option ROM: 18.1.1.5201
- AHCI Code: ACHI_24
- LAN i225-V Option ROM: 0.9.02
- Visual BIOS: Intel AptioV

- Supported Flash Devices:
    - WinBond W25Q256JV 32MB
    - GigaDevice GD25B256D 32MB

- Microcode Updates included in .BIN & .CAP Files:
    - MC2806D1_00000050.pdb

Feature Changes/Updates/Fixes:

- Fixed issue where Image Parser Corruption Vulnerability
- Updated 2023.4 Intel Platform Update
- Updated 2024.1 Intel Platform Update
- Fixed issue where UsbRt TOCTOU Vulnerability
- Fixed issue where Flash driver security review
- Fixed issue where Extended Image Parser Corruption Correction
- Fixed issue where Vulnerabilities in EDK2 NetworkPkg

Known Errata:

- Windows Bitlocker Recovery will appear if Secure Boot Key is re-loaded in BIOS Setup when on KC0044.

BIOS Version 0047 - KCTGL357.0047.2023.1226.1705

About This Release:

- Date: Dec 26, 2023
- ROM Image Checksum: 0XAA9552E9
- EC Firmware: 1.15.09.000
- ME Firmware: 15.0.47.2473
- PCH Configuration Firmware: 15.0.0.1021
- PMC Firmware: 150.2.10.1020
- iTBT Firmware: 15.0.0.0311
- IOM Firmware: 24.31.0.0000
- Retimer Firmware in BIOS capsule: 2.22
- NPHY Firmware: 15.107.135.5018
- CRB Label: 1AWHY_048
- Boot Guard ACM: 1.14.46
- BIOS Guard: BiosGuard_029
- Silicon Initialization Code: 0A.00.5D.32(4303.02)
- Memory Reference Code: 2.0.2.8
- Integrated Graphics:
    - UEFI Driver: 17.0.1070
- Intel RST Pre-OS:
    - VMD Option ROM: 18.1.1.5201
- AHCI Code: ACHI_24
- LAN i225-V Option ROM: 0.9.02
- Visual BIOS: Intel AptioV

- Supported Flash Devices:
    - WinBond W25Q256JV 32MB
    - GigaDevice GD25B256D 32MB

- Microcode Updates included in .BIN & .CAP Files:
    - MC2806D1_00000050.pdb

Feature Changes/Updates/Fixes:

- Updated Intel KEK/DB keys to support MSFT CA 2023
- Fixed issue where LogoFAIL Vulnerability
- Fixed issue where UsbSmmRt vulnerability
- Updated NetworkPkg EDK2
- Fixed issue where EDK2 PEI-Phase Denial of Service Vulnerability
- Fixed issue where Intel NUC TOCTOU vulnerability
- Fixed issue where TOCTOU Vulnerability in SmiFlash
- Updated ME to 15.0.47.2473
- Updated CPU Microcode to MC2806D1_00000050.pdb
- Fixed issue where The values of IsetupCfg password check setting cannot be kept when press save icon on upper right corner.

Known Errata:

- Windows Bitlocker Recovery will appear if Secure Boot Key is re-loaded in BIOS Setup when on KC0044.

BIOS Version 0045 - KCTGL357.0045.2023.0519.1140

About This Release:

- Date: May 19, 2023
- ROM Image Checksum: 0XAAAE3515
- EC Firmware: 1.15.09.000
- ME Firmware: 15.0.45.2411
- PCH Configuration Firmware: 15.0.0.1021
- PMC Firmware: 150.2.10.1020
- iTBT Firmware: 15.0.0.0311
- IOM Firmware: 24.31.0.0000
- Retimer Firmware in BIOS capsule: 2.22
- NPHY Firmware: 15.107.135.5018
- CRB Label: 1AWHY_048
- Boot Guard ACM: 1.14.46
- BIOS Guard: BiosGuard_029
- Silicon Initialization Code: 0A.00.5D.32(4303.02)
- Memory Reference Code: 2.0.2.8
- Integrated Graphics:
    - UEFI Driver: 17.0.1070
- Intel RST Pre-OS:
    - VMD Option ROM: 18.1.1.5201
- AHCI Code: ACHI_24
- LAN i225-V Option ROM: 0.9.02
- Visual BIOS: Intel AptioV

- Supported Flash Devices:
    - WinBond W25Q256JV 32MB
    - GigaDevice GD25B256D 32MB

- Microcode Updates included in .BIN & .CAP Files:
    - MC2806D1_00000046.pdb

Feature Changes/Updates/Fixes:

- Fixed issue where “TOCTOU” vulnerability.
- Fixed issue where EDK2 vulnerabilities.
- Fixed issue where OOB RW vulnerabilitity.
- Added PlatformLang Timeout Variable Access.
- Fixed issue where SmmEntryPoint Underflow vulnerability.
- Fixed issue where UEFI Variable access vulnerability.
- Fixed issue where OpenSSL vulnerabilities.
- Updated IPU 2023.2.
- Updated IPU 2023.1.
- Updated EC FW to 1.15.09.000.
- Added NEW Feature: "Set Virtual Numpad to non-functional" implemented.
- Updated ME FW to 15.0.45.2411 (V2)
- Updated CPU Microcode to MC2806D1_00000046.pdb.
- Fixed issue where When the Intel i219 LAN and Thunderbolt support items are disabled in the BIOS, the system cannot update the BIOS through the Power Button Menu “[F7] Update BIOS” option.

Known Errata:

- Windows Bitlocker Recovery will appear if Secure Boot Key is re-loaded in BIOS Setup when on KC0044.

BIOS Version 0044 - KCTGL357.0044.2023.0130.1106

About This Release:

- Date: 01/30/2023
- ROM Image Checksum: 0XAAC1A872
- EC Firmware: 1.14.09.000
- ME Firmware: 15.0.41.2158
- PCH Configuration Firmware: 15.0.0.1021
- PMC Firmware: 150.2.10.1020
- iTBT Firmware: 15.0.0.0045
- IOM Firmware: 24.31.0.0000
- Retimer Firmware in BIOS capsule: 2.22
- NPHY Firmware: 15.107.135.5017
- CRB Label: 1AWHY_048
- Boot Guard ACM: 1.14.39
- Bios Guard: BiosGuard_029
- Silicon Initialization Code: 0A.00.5D.32(4303.02)
- Memory Reference Code: 2.0.2.8
- Integrated Graphics:
    - UEFI Driver: 17.0.1070
- Intel RST Pre-OS:
    - VMD Option ROM: 18.1.1.5201
- AHCI Code: ACHI_24
- LAN i225-V Option ROM: 0.9.02
- Visual BIOS: Intel AptioV

- Supported Flash Devices:
    - WinBond W25Q256JV 32MB
    - GigaDevice GD25B256D 32MB

- Microcode Updates included in .BIN & .CAP Files:
    - MC2806D1_00000042.pdb

Feature Changes/Updates/Fixes:

- Fixed issue where SDIO_DEV_CONFIGURATION SetVariable NVRAM Corruption.
- Fixed issue where OS Kernel-level malware may cause information disclosure vulnerability.
- Fixed issue where UEFI Boot Variables Access.
- Added BIOS WU setup support added.
- Fixed issue where BIOS Password Entry Points_F8 hot key.
- Updated Building Process optimize_avoid UQI duplicated.

Known Errata:

- Windows Bitlocker Recovery will appear if Secure Boot Key is re-loaded in BIOS Setup when on KC0044.

BIOS Version 0043 - KCTGL357.0043.2022.1021.2047

About This Release:

- Date: 10/21/2022

- ROM Image Checksum: 0xAAD8327F
- EC Firmware: 1.14.09.000
- ME Firmware: 15.0.41.2158
- PCH Configuration Firmware: 15.0.0.1021
- PMC Firmware: 150.2.10.1020
- iTBT Firmware: 15.0.0.0045
- IOM Firmware: 24.31.0.0000
- Retimer Firmware in BIOS capsule: 2.22
- NPHY Firmware: 15.107.135.5017
- Boot Guard ACM: 1.14.39
- Bios Guard: BiosGuard_029
- Silicon Initialization Code: 0A.00.5D.32(4303.02)
- Memory Reference Code: 2.0.2.8
- Integrated Graphics:
    - UEFI Driver: 17.0.1070
- Intel RST VMD:
    - VMD Option ROM: 18.1.1.5201
- AHCI Code: AHCI_24
- LAN i225-V Option ROM: 0.9.02
- Visual BIOS: Intel AptioV

- Supported Flash Devices:
    - WinBond W25Q256JV 32MB
    - GigaDevice GD25B256D 32MB

- Microcode Updates included in .BIN & .CAP Files:
    - MC2806D1_00000042.pdb

New Fixes/Features:

- Fixed issue where GRUB Bootloader Vulnerability.
- Fixed issue where Intel NUC information disclosure vulnerability.
- Fixed issue where Intel NUC vulnerability/Intel info leak vulnerability.
- Updated 2022 IPU update: 2022.1/2022.2/2022.3.
- Updated ME FW to 15.0.41.2158.
- Fixed issue where Potential hack of Intel BIOS EBU DLL.
- Fixed issue where SIO_DEV_STATUS_VAR_NAME Information Leakage_PTK2712#12.
- Fixed issue where RSB Stuffing Mitigation for Speculative Execution Vulnerability.
- Fixed issue where UEFI Variable access vulnerability in Intel NUC BIOS.
- Added Implement S3 Reboot code in MS support project.
- Fixed issue where PEI memory corruption on server boards and on a majority of Intel NUCs.
- Fixed issue where Fixes for TianoCore Security Issues.
- Added Variable Struct Counter.
- Fixed issue where iSetupCfg tool not able to change default value of “PLx/Fan” curve parameters due to “stdDefault” override mechanism.
- Added “StdDefaults” into “ProtectedNvVariableForRuntime” ELink.
- Fixed issue where System BIOS could not restore USB functionality after disabling all the USB ports in the BIOS Setup USB sub-menu.

BIOS Version 0042 - KCTGL357.0042.2022.0727.1604

About This Release:

- Date: Jul 27 2022
- ROM Image Checksum: 0xAAFB058F
- ME Firmware: Consumer 15.0.35.1898
- EC Firmware: 1.14.09.000
- PMC Firmware: 150.2.10.1019
- Boot Guard ACM: 1.14.23
- Reference Code: Based on 0A.00.5D.32
- Memory Reference Code: Based on 2.0.2.8
- Integrated Graphics:
  - UEFI Driver: 17.0.1070
- Intel RST VMD:
  - VMD Option ROM: 18.1.1.5201
- LAN i225-V Option ROM: 0.9.02
- Visual BIOS: Intel AptioV

- Supported Flash Devices:
  - WinBond W25Q256FV 32MB
  - GigaDevice GD25B256D 32MB

- Microcode Updates included in .BIN & .CAP Files:
  - MC2806D1_0000003C.pdb

New Fixes/Features:

- Fixed issue where POST hotkey message do not display with Secure Boot enabled.
- Fixed issue where BootPerformanceTable_pointer.
- Fixed issue where SMM memory corruption vulnerability in SMM driver on Intel platforms.
- Fixed issue when Stack overflow vulnerability in SMI handler.
- Fixed issue where Privilege escalation vulnerability from kernel to SMM in multiple devices.
- Fixed issue where the arbitrary code execution in DXE driver.
- Fixed issue where Optimize F6 string layout patch, fix for letters 'y' and 'g' will get truncated by the next line.
- Added ME FW minor version checking algorithm.
- Added Message warning when a BIOS upgrade means a downgrade is no possible. This has been defined in BIOS_Master_RD_v3.10.01.
- Added BIOS Warning message displayed during BIOS WU update.
- Fixed issue where Correct EC MMIO Driver (ACPI memory resource RangeLength) to 0x100.
- Fixed issue where for Intel NUC information leak vulnerability.
- Fixed issue where for Fastboot Getvariable 4th parameter(size) has a risk of being attacked.
- Fixed issue where Arbitrary write vulnerability in PEI module leads to arbitrary code execution in PEI phase.
- Fixed issue where fTPM does not function after RTC power loss.
- Fixed issue where system will always reset loop after RTC power loss.
- Fixed issue where The stack buffer overflow vulnerability leads to arbitrary code execution in DXE driver.
- Fixed issue where for Buffer overflow in UEFI Firmware BIOS core.

- Updated EC FW binary to 1.14.09.000.

BIOS Version 0040 - KCTGL357.0040.2021.1126.1843

About This Release:

- Date: Nov 26, 2021
- ROM Image Checksum: 0xAAF76A29
- ME Firmware: Consumer 15.0.35.1898
- EC Firmware: 1.11.09.000
- PMC Firmware: 150.2.10.1019
- Boot Guard ACM: 1.14.23
- Reference Code: Based on 0A.00.5D.32
- Memory Reference Code: Based on 2.0.2.8
- Integrated Graphics:
  - UEFI Driver: 17.0.1070
- Intel RST VMD:
  - VMD Option ROM: 18.1.1.5201
- LAN i225-V Option ROM: 0.9.02
- Visual BIOS: Intel AptioV

- Supported Flash Devices:
  - WinBond W25Q256FV 32MB
  - GigaDevice GD25B256D 32MB

- Microcode Updates included in .BIN & .CAP Files:
  - MC2806D1_0000003C.pdb

New Fixes/Features:

- Added Functionality for Whisper Mode.
- Updated issues with Hardware Security Testability Interface Test.
- Updated EC Firmware version to 1.11.09.000.
- Fixed issue with BIOS update after updating to Win 11.
- Fixed issue with D20/F2 SVID/SSID setting not being set.
- Added undervolting support setup item.
- Fixed issue where PXE Boot failed to show WDS Boot Manager screen.
- Fixed issue where keyboard did not function in BIOS Setup occasionally.

BIOS Version 0038 - KCTGL357.0038.2021.0806.2133

About This Release:

- Date: Aug 06, 2021
- ROM Image Checksum: 0xAB278392
- ME Firmware: 15.0.30.1776
- EC Firmware: 1.07.09.000
- PMC Firmware: 150.2.10.1017
- Boot Guard ACM: 1.14.20
- Reference Code: Based on 0A.00.54.31
- Memory Reference Code: Based on 2.0.2.6
- Integrated Graphics:
  - UEFI Driver: 17.0.1061
- Intel RST VMD:
  - VMD Option ROM: 18.1.1.5201

- LAN i225-V Option ROM: 0.9.02
- Visual BIOS: Intel AptioV

- Supported Flash Devices:
  - WinBond W25Q256FV 32MB
  - GigaDevice GD25B256D 32MB

- Microcode Updates included in .BIN & .CAP Files:
  - MC2806D1_00000032.pdb

New Fixes/Features:

- Updated EC Firmware to 1.07.09.000

BIOS Version 0037 - KCTGL357.0037.2021.0712.0948

About This Release:

- Date: July 12, 2021
- ROM Image Checksum: 0xAB28CB4D
- ME Firmware: Consumer 15.0.30.1776
- EC Firmware: 1.05.09.000
- PMC Firmware: 150.2.10.1017
- Boot Guard ACM: 1.14.20
- Reference Code: Based on 0A.00.54.31
- Memory Reference Code: Based on 2.0.2.6
- Integrated Graphics:
  - UEFI Driver: 17.0.1061
- Intel RST VMD:
  - VMD Option ROM: 18.1.1.5201
- Supported Flash Devices:
  - WinBond W25Q256FV 32MB
  - GigaDevice GD25B256D 32MB
- Microcode Updates included in .BIN & .CAP Files:
  - MC2806D1_00000032.pdb

New Fixes/Features:

- Initial production BIOS release.

LEGAL INFORMATION