

EIN No: SSDCMY-018 Rev. A Date: April 11, 2025 Originator: Enterprise SSD Product Group 1

Engineering Information Notice (EIN)

PRODUCT AFFECTED

For Generic, Non-SED, KCMY series (2.5 inch)

KCMY1RUGxxxx Series: 1 DWPD
KCMY1RUG1T92: SDF7005GEAxxx
KCMY1RUG3T84: SDF7004GEAxxx
KCMY1RUG7T68: SDF7003GEAxxx
KCMY1RUG15T3: SDF7001GEAxxx
KCMY1RUG30T7: SDF7000GEAxxx

KCMY1VUGxxxx Series: 3DWPD
KCMY1VUG1T60: SDF7Y05GEAxxx
KCMY1VUG3T20: SDF7Y04GEAxxx
KCMY1VUG6T40: SDF7Y03GEAxxx
KCMY1VUG12T8: SDF7Y01GEAxxx

For Generic, SIE, KCMY series (2.5 inch)

KCMYXRUGxxxx Series: 1 DWPD
KCMYXRUG1T92: SDF7085GEBxxx
KCMYXRUG3T84: SDF7084GEBxxx
KCMYXRUG7T68: SDF7083GEBxxx
KCMYXRUG15T3: SDF7081GEBxxx
KCMYXRUG30T7: SDF7080GEBxxx

KCMYXVUGxxxx Series: 3 DWPD
KCMYXVUG1T60: SDF7Y85GEBxxx
KCMYXVUG3T20: SDF7Y84GEBxxx
KCMYXVUG6T40: SDF7Y83GEBxxx
KCMYXVUG12T8: SDF7Y81GEBxxx

For Generic, SED, KCMY series (2.5 inch)

KCMYDRUGxxxx Series: 1 DWPD
KCMYDRUG1T92: SDF7045GEBxxx
KCMYDRUG3T84: SDF7044GEBxxx
KCMYDRUG7T68: SDF7043GEBxxx
KCMYDRUG15T3: SDF7041GEBxxx
KCMYDRUG30T7: SDF7040GEBxxx

KCMYDVUGxxxx Series: 3 DWPD
KCMYDVUG1T60: SDF7Y45GEBxxx
KCMYDVUG3T20: SDF7Y44GEBxxx
KCMYDVUG6T40: SDF7Y43GEBxxx
KCMYDVUG12T8: SDF7Y41GEBxxx

For Generic, FIPS, KCMY series (2.5 inch)

KCMYFRUGxxxx Series: 1 DWPD
KCMYFRUG1T92: SDF7065GEBxxx
KCMYFRUG3T84: SDF7064GEBxxx
KCMYFRUG7T68: SDF7063GEBxxx
KCMYFRUG15T3: SDF7061GEBxxx
KCMYFRUG30T7: SDF7060GEBxxx

KCMYFVUGxxxx Series: 3 DWPD
KCMYFVUG1T60: SDF7Y65GEBxxx
KCMYFVUG3T20: SDF7Y64GEBxxx
KCMYFVUG6T40: SDF7Y63GEBxxx
KCMYFVUG12T8: SDF7Y61GEBxxx

ENGINEERING INFORMATION NOTICE

CLASSIFICATION

- Electrical
- Mechanical
- Others

LEVEL

- Hardware
- Software (firmware)
- Document
- Manufacturing
- Others

IMPLEMENTATION

- Factory
- Customer side
- As required
- Repaired
- Retrofit kit required

PRIORITY

- Urgent
- Immediate
- Routine

REVISION LEVEL

For Generic, Non-SED, KCMY series (2.5 inch)

KCMY1RUGxxxx Series: 1 DWPD

KCMY1RUG1T92: SDF7005GEAxxx

Item	Current	Revised
EC Rev.	A2	A3
FW Rev.	1UET6104	1UET6106

KCMY1RUG3T84: SDF7004GEAxxx

Item	Current	Revised
EC Rev.	A2	A3
FW Rev.	1UET6104	1UET6106

KCMY1RUG7T68: SDF7003GEAxxx

Item	Current	Revised
EC Rev.	A2	A3
FW Rev.	1UET6104	1UET6106

KCMY1RUG15T3: SDF7001GEAxxx

Item	Current	Revised
EC Rev.	A2	A3
FW Rev.	1UET6104	1UET6106

KCMY1RUG30T7: SDF7000GEAxxx

Item	Current	Revised
EC Rev.	A2	A3
FW Rev.	1UET6104	1UET6106

KCMY1VUGxxxx Series: 3DWPD

KCMY1VUG1T60: SDF7Y05GEAxxx

Item	Current	Revised
EC Rev.	A2	A3
FW Rev.	1UET6104	1UET6106

KCMY1VUG3T20: SDF7Y04GEAxxx

Item	Current	Revised
EC Rev.	A2	A3
FW Rev.	1UET6104	1UET6106

KCMY1VUG6T40: SDF7Y03GEAxxx

Item	Current	Revised
EC Rev.	A2	A3
FW Rev.	1UET6104	1UET6106

KCMY1VUG12T8: SDF7Y01GEAxxx

Item	Current	Revised
EC Rev.	A2	A3
FW Rev.	1UET6104	1UET6106

ENGINEERING INFORMATION NOTICE

For Generic, SIE, KCMY series (2.5 inch)

KCMYXRUGxxxx Series: 1 DWPD
KCMYXRUG1T92: SDF7085GEBxxx

Item	Current	Revised
EC Rev.	A2	A3
FW Rev.	1UETE104	1UETE106

KCMYXRUG7T68: SDF7083GEBxxx

Item	Current	Revised
EC Rev.	A2	A3
FW Rev.	1UETE104	1UETE106

KCMYXRUG30T7: SDF7080GEBxxx

Item	Current	Revised
EC Rev.	A2	A3
FW Rev.	1UETE104	1UETE106

KCMYXVUGxxxx Series: 3 DWPD
KCMYXVUG1T60: SDF7Y85GEBxxx

Item	Current	Revised
EC Rev.	A2	A3
FW Rev.	1UETE104	1UETE106

KCMYXVUG6T40: SDF7Y83GEBxxx

Item	Current	Revised
EC Rev.	A2	A3
FW Rev.	1UETE104	1UETE106

KCMYXRUG3T84: SDF7084GEBxxx

Item	Current	Revised
EC Rev.	A2	A3
FW Rev.	1UETE104	1UETE106

KCMYXRUG15T3: SDF7081GEBxxx

Item	Current	Revised
EC Rev.	A2	A3
FW Rev.	1UETE104	1UETE106

KCMYXVUG3T20: SDF7Y84GEBxxx

Item	Current	Revised
EC Rev.	A2	A3
FW Rev.	1UETE104	1UETE106

KCMYXVUG12T8: SDF7Y81GEBxxx

Item	Current	Revised
EC Rev.	A2	A3
FW Rev.	1UETE104	1UETE106

For Generic, SED, KCMY series (2.5 inch)

KCMYDRUGxxxx Series: 1 DWPD
KCMYDRUG1T92: SDF7045GEBxxx

Item	Current	Revised
EC Rev.	A2	A3
FW Rev.	1UET7104	1UET7106

KCMYDRUG7T68: SDF7043GEBxxx

Item	Current	Revised
EC Rev.	A2	A3
FW Rev.	1UET7104	1UET7106

KCMYDRUG30T7: SDF7040GEBxxx

Item	Current	Revised
EC Rev.	A2	A3
FW Rev.	1UET7104	1UET7106

KCMYDRUG3T84: SDF7044GEBxxx

Item	Current	Revised
EC Rev.	A2	A3
FW Rev.	1UET7104	1UET7106

KCMYDRUG15T3: SDF7041GEBxxx

Item	Current	Revised
EC Rev.	A2	A3
FW Rev.	1UET7104	1UET7106

ENGINEERING INFORMATION NOTICE

KCMYDVUGxxxx Series: 3 DWPD

KCMYDVUG1T60: SDF7Y45GEBxxx

Item	Current	Revised
EC Rev.	A2	A3
FW Rev.	1UET7104	1UET7106

KCMYDVUG6T40: SDF7Y43GEBxxx

Item	Current	Revised
EC Rev.	A2	A3
FW Rev.	1UET7104	1UET7106

KCMYDVUG3T20: SDF7Y44GEBxxx

Item	Current	Revised
EC Rev.	A2	A3
FW Rev.	1UET7104	1UET7106

KCMYDVUG12T8: SDF7Y41GEBxxx

Item	Current	Revised
EC Rev.	A2	A3
FW Rev.	1UET7104	1UET7106

For Generic, FIPS, KCMY series (2.5 inch)

KCMYFRUGxxxx Series: 1 DWPD

KCMYFRUG1T92: SDF7065GEBxxx

Item	Current	Revised
EC Rev.	A2	A3
FW Rev.	1UETP104	1UETP106

KCMYFRUG7T68: SDF7063GEBxxx

Item	Current	Revised
EC Rev.	A2	A3
FW Rev.	1UETP104	1UETP106

KCMYFRUG30T7: SDF7060GEBxxx

Item	Current	Revised
EC Rev.	A2	A3
FW Rev.	1UETP104	1UETP106

KCMYFRUG3T84: SDF7064GEBxxx

Item	Current	Revised
EC Rev.	A2	A3
FW Rev.	1UETP104	1UETP106

KCMYFRUG15T3: SDF7061GEBxxx

Item	Current	Revised
EC Rev.	A2	A3
FW Rev.	1UETP104	1UETP106

KCMYFVUGxxxx Series: 3 DWPD

KCMYFVUG1T60: SDF7Y65GEBxxx

Item	Current	Revised
EC Rev.	A2	A3
FW Rev.	1UETP104	1UETP106

KCMYFVUG6T40: SDF7Y63GEBxxx

Item	Current	Revised
EC Rev.	A2	A3
FW Rev.	1UETP104	1UETP106

KCMYFVUG3T20: SDF7Y64GEBxxx

Item	Current	Revised
EC Rev.	A2	A3
FW Rev.	1UETP104	1UETP106

KCMYFVUG12T8: SDF7Y61GEBxxx

Item	Current	Revised
EC Rev.	A2	A3
FW Rev.	1UETP104	1UETP106

Special Attention for FW-download

To Enable items that described "Need power cycle" in "Category" Column, it is necessary power cycle to update 1UETx106 Firmware from 1UETx104 or before as follows.
The first download may take around 3.5 seconds.

```
Firmware update command sequence
# nvme id-ctrl $DeviceName ; check FW revision
# nvme fw-download $DeviceName --fw=***(Describe new Firmware name)
# nvme fw-commit $DeviceName --action=3
# nvme id-ctrl $DeviceName; check FW revision
Wait about 10 seconds.
Power cycle.
```

DESCRIPTION OF CHANGE

1. Fixed issues:

(1) Sanitize

Issue: In the security drive, such as SED or FIPS, once the Sanitize Block Erase with AUSE=0 (restricted completion mode) is failed, the drive cannot accept subsequent Sanitize Crypt Erase with AUSE=0 for recovery.

Cause: When Sanitize Block Erase with AUSE=0 is failed, the failure recovery step is required. To do the recovery, but the subsequent Sanitize Crypt Erase with AUSE=0 is not accepted because of the FW problem.

Fix: The drive FW is modified to accept subsequent Sanitize Crypt Erase with AUSE=0 for recovery.

Severity: Middle

Likelihood: Low

(2) LBA Status Information Attributes feature

Issue: The DWORD-0 of the CQ (completion Queue) for SetFeature command for LBA Status Information Attribute (FID=15h) should have the FID=15h current value, but report all zero.

Cause: FW implementation error not to report the current value in the DWORD-0 of the CQ. Spec violation.

Fix: The FW is fixed to report correct value of the FID=15h in the DWORD-0 of the CQ.

Severity: Low

Likelihood: High

(3) Sanitize Status Log-page

Issue: SCDW10 (Sanitize Command Dword-10 Information) field in the Sanitize Status Log-page (LID=81h) is NOT updated correctly.

Cause: FW implementation error. In case of sanitize failure recovery, SCDW10 in Sanitize Status Log-page is not updated expectedly.

Fix: Updated SCDW10 field in Sanitize Status Log-page (LID 0x81h) for Exit Failure mode in case of sanitize failure recovery.

Severity: Low

Likelihood: High

(4) Command timeout

Issue: Command timeout occurs when Controller Reset is executed during multiple NS Delete are requested.

Cause: Internal information to monitor NS delete completion is incorrectly calculated when previous NS Delete is still in progress.

Fix: Corrected calculation of Internal information to monitor NS delete by considering the status of the ongoing NS delete.

Severity: Middle

Likelihood: Middle

(5) NS detach

Issue: For Private NS, the NS Detach Command fails when it is issued from the Controller to which NS is not attached.

Cause: Code implementation was wrong.

Fix: Removed the existing check and hence, Private NS Detach Command succeeds whenever it is issued from the Controller to which that respective Private NS is not attached.

Severity: Low

Likelihood: High

(6) Sanitize

Issue: All Admin commands except sanitize command are passed after recent sanitize operation has failed.

Cause: No conditional check is present in case sanitize failed for admin command.

Fix: Only specific Admin commands allowed during sanitize are executed when sanitize command fails.

Severity: Low

Likelihood: High

(7) MCTP over SMBus

Issue: When receiving a Set Endpoint ID via SMBus from a different Source EID, the drive incorrectly responded with Accept instead of Reject.

Cause: The Set Endpoint ID process did not include a step to compare the Source EID of the newly received Set Endpoint ID with the Source EID of the previous one.

Fix: Add a step to compare the Source EID of the previously received Set Endpoint ID with the Source EID of the newly received one.

Severity: Low

Likelihood: High

(8) IO command timeout

Issue: The host IO commands may hang if reset is received in the middle of IO execution. The drive will recover with a power cycle.

Cause: The drive HW expects all IO commands on the fly should be processed when the drive internal Reset operation is complete. However, there is a small time window to have some pending IO command in process when the internal Reset process is completed. The drive FW detects this situation then FW assert happened.

Fix: When the drive HW has completed Reset process but there is an IO command being executed, the drive FW is modified to wait until the IO command is completed.

Severity: Middle

Likelihood: Low

(9) Set feature FID 81h

Issue: After setting the Host Identifier by the SetFeaturer FID=81h, if the Current and Saved values are different, FW Assert may occur after FW Activation with CC.CRIME=1. It is easy to occur when FW Activate is performed in a power cycle, and it is not recovered even in a power cycle.

Cause: In the process of copying the saved value of HOST ID to the current value after FW Activation, the value may be copied to the prohibited period of internal information update, and FW Assert occurred.

Fix: FW was modified to avoid copying during the period when internal information update is prohibited.

Severity: High

Likelihood: Middle

(10) TCG transaction abort

Issue: TCG transaction abort process may cause Assert and failure when issued. Power cycle cannot recover.

Cause: When the TCG transaction abort is executed, the TCG-related data is rewound, but if non-volatilization of internal management information occurs during the rewinding process, FW is asserted due to an internal resource conflict.

Fix: TCG-related data rewind process and non-volatilization of internal management information are now exclusive.

Severity: High

Likelihood: Low

(11) DRAM (Need power cycle)

Issue: If the drive contains a DRAM from the specific supplier, the drive may detect DRAM data corruption during normal host IO operations. When this DRAM corruption is detected, then the drive stops the operation. The drive cannot be recovered with a power cycle.

Cause: During the DRAM data reading, there is a small time window to start reading the DRAM data at the wrong timing, resulting in a data offset shifted in a few cycle. When the drive detects DRAM data corruption, the drive stops the operation immediately to prevent wrong user-data sending back to the host.

Fix: The DRAM signal configuration is modified to eliminate the timing where the DRAM data is mistakenly read at the wrong timing. This new configuration set-up is applied only for this specific DRAM supplier for newly shipping drive only. This countermeasure does not impact any performance of the DRAM access.

Severity: High

Likelihood: Middle

(12) Read for trimmed LBAs

Issue: Read performance for Trimmed LBAs is limited to about 7400MB/s Seq.R in Gen.5 environment.

Cause: The bandwidth of internal transfer of read data for Trimmed LBAs was not sufficient.

Fix: Increased the bandwidth of internal transfer of read data for Trimmed LBAs and increased the performance to 13800MB/s.

Severity: Middle

Likelihood: High

(13) Persistent Event Log

Issue: There is a case where a previously reported Persistent Event Log is reported again.

Cause: After CC.EN=1, the proper saving process for the temporarily stored logs is performed, but there is a possibility that logs previously read with the Get Log Page (Persistent Event Log) command are recorded again.

Fix: In the proper saving process for the temporarily stored logs after CC.EN=1, only the temporarily stored logs are recorded, and the logs read with the Get Log Page command are not recorded.

Severity: Low

Likelihood: Middle

(14) PCI info in PERST mode

Issue: PCI information of the drive is being cleared as soon as PERST is asserted. The expected behavior is that the bus/device number would change but all other information stays the same.

Cause: FW sets PCI Vendor ID, etc. to HW at drive initialization. When BDF is assigned by Host, HW remembers it. When Read NVMe-MI Data Structure is executed, FW obtains PCI information, such as BDF and PCI Vendor ID, from HW. During PERST, FW returned All 0x00 because the HW is reset and the FW cannot get information from HW. BDF is initialized to 0 after PERST, so 0 response is fine, but other PCI information should not have returned 0.

Fix: For PCI Information such as PCI Vendor ID other than BDF, FW also keeps their value. So, fixed to respond the value directly from FW instead of getting them from HW.

Severity: Low

Likelihood: Middle

(15) NVMe-MI

Issue: When the MCTP-MI was intentionally paused by the host, the drive does NOT set SOM (Start of Message) =1b on the next packed resumed by the Replay command.

Cause: FW implementation error not to set SOM=1 in this situation. Spec violation.

Fix: FW is modified to set SOM=1b in this situation.

Severity: Middle

Likelihood: Low

(16) Die offline

Issue: When die offline occurs and the following workload is executed during die offline recovery, BE may be asserted.
Condition: drive capacity = 1.92TB~15TB, workload: Host read + Host write

Cause: When a Flash Die went offline and then a Read and Write access occurred to another non-Offline Die, the normal Die was incorrectly determined to be the Offline Target Die, and the necessary process could not be performed correctly when Read/Write accesses occurred at the same time. As a result, subsequent Read commands for that Die were not executed correctly and a timeout occurred, caused a FW Assert.

Fix: When both Read and Write accesses occurred at the same time, the Die offline target Die was not judged incorrectly.

Severity: High

Likelihood: Low

(17) MSI-X

Issue: When MSI-X error is detected, the error log entry of the drive is mistakenly incremented.

Cause: It is miss-implementation of the PCIe spec. The drive mistakenly increments the error log entry when the MSI-X error is detected.

Fix: When the drive detects MSI-X error, there is no Asynchronous Event (Transient Internal Error) reported.

Severity: Low

Likelihood: High

(18) FLR during NSSR

Issue: If FLR is executed during NSSR processing, the Admin command times out after NSSR completion.

Cause: If FLR is executed between NSSR post-processing and reset interrupt status clearing, FLR is executed and FLR Status is set on the HW side, but FLR processing is skipped on the FW side because NSSR is in progress. The FLR status is not cleared in the post-processing of the NSSR, so the FLR status set by the HW remains in place and the command cannot be fetched, resulting in a timeout.

Fix: Clear FLR Status in NSSR post-processing.

Severity: Middle

Likelihood: Low

(19) FW D/L

Issue: When FW Commit command is executed with CA=1 or 2, and waiting for a Reset to activate it, then followed by the another FW Commit command with CA=3 is received. During this activation, if Reset is received, then the drive gets hang-up.

Cause: During the FW activation for CA=3, the drive FW did not care about the activation trigger either Reset (CA=1 or 2) or on-line activation (CA=3). Unexpected Reset cannot handle correctly in this situation, resulting the drive hang condition.

Fix: Add a check routine if the firmware is already being activated by Reset or online update.

Severity: Middle

Likelihood: Low

(20) Reservation command

Issue: When using a specific revision of the Linux kernel, issuing the Reservation Register command from the nvme cli may cause the cli to hang without responding.

Cause: The Drive is able to execute the command and there is no abnormality, but the attribute value of the Reservation system command reported in Get Log Page LID=05h is considered to be the cause of the hang.

Fix: Change Command Submission and Execution (CSE) and Namespace Capability Change (NCC) from 1 to 0 in the reported value of Reservation Register, Acquire, Release in LID=05h.

Severity: Middle

Likelihood: Middle

(21) FW commitment

Issue: The FW Commit command may not complete if Reset occurs during the process of FW activation.

Cause: When a reset is received during the FW activation process, the activation process waits for the completion of Reset. At the same time, the Reset process waits for the FW activation completion. The drive may fall into the deadlock situation, resulting the FW Commit command timeout.

Fix: Fix the drive FW not to wait for FW activation completion in this situation.

Severity: Middle

Likelihood: Low

(22) IO command timeout

Issue: IO command timeout may be detected due to the inconsistent internal conditions. The drive power cycle does not recover this failure.

Cause: During the normal drive operation, multiple superblocks are programmed at the same time, but when the drive internal user-data recovery was invoked, there is a timing to stop supplying the single superblock. When the drive power is lost at this time, the superblock management information becomes inconsistent, and this causes FW assert.

Fix: Changed that superblock management information not to be inconsistent even if the above situation occurs.

Severity: High

Likelihood: Low

(23) NVM Format command (SIE, SED, and FIPS only)

Issue: When the host Rd/Wr CMDs are executed, and if the NVM Format CMD (SES=0) to another Namespace is issued, then the FW assert happens and the drive falls into the failure mode.

Cause: The NVM Format CMD operation for no secure operation (SES=0) will access the specific HW module. However, the host Rd/Wr operation for another Namespace also uses the same HW module, which conflicts with each other. The drive FW detects this situation and stops the operation by asserting the FW.

Fix: When The NVM Format CMD operation needs to access the HW module, the drive FW intentionally suspends the usual host Rd/Wr operation internally to prevent conflicting accesses.

Severity: Middle

Likelihood: Low

(24) FLR and Warm Reset

Issue: Link Up may not be performed by Warm reset immediately after Function Level Reset (FLR).

Cause: When Warm reset (PERST# Assert) is received immediately after FLR is received, FLR processing may be completed before PERST# Assert event processing is completed.

The mask of unnecessary interrupts was set at the start of PERST# Assert processing, but the mask was released at the completion of FLR processing. As a result, the FW hung up because it was unable to respond to interrupts that occurred during PERST# Assert event processing because they were unexpected.

Fix: When PERST# Assert event processing is in progress at the time of FLR processing completion, the Mask of the interrupts is not released.

Severity: Middle

Likelihood: Middle

(25) Error Recovery feature

Issue: If DULBE (Deallocated or Unwritten Logical Block Error) bit is set, issuing Compare command to an unallocated LBA failed with Compare error.

Cause: If DULBE bit is set, Compare command for an unallocated LBA should fail with UNALLOC_BLOCK error on NVMe spec, but failed with COMPARE_FAILED.

Fix: Fixed that Compare command for unassigned LBAs fail with UNALLOC_BLOCK error if the DULBE bit is set.

Severity: Middle

Likelihood: Middle

(26) Recovery from Forced Assert

Issue: After sanitize failed, Format command aborted to recover the drive from forced assert.

Cause: Format is not allowed when sanitize has failed.

Fix: Allow Format command in the state of forced assert even if sanitize has failed.

Severity: Low

Likelihood: Middle

(27) Command timeout

Issue: If a reset is received from both ports simultaneously while the drive is executing IO command fetches on both ports in parallel, IO may become unresponsive after the reset process. If the reset is received again from the host in this state, the reset process will not be completed and the drive will go offline. The only recovery method is a power cycle.

Cause: In CM7, the number of DMACs for IO command fetching has been increased from one to three. When multiple DMACs stopped simultaneously due to errors, there were cases where the FW could not correctly clear the error status of the DMACs. The error status of the DMACs remained unexpectedly, so the HW could not start the next DMAC. This occurred when one port stopped with a non-fatal error (e.g., link error) and retried DMAC transfer, while the other port stopped with a reset factor and drop the transfer request.

Fix: Fixed to correctly clear DMAC error status even when multiple DMACs stop simultaneously due to errors.

Severity: Middle

Likelihood: Low

(28) Drive Failure

Issue: There is a risk of PLP process failure if a power loss occurs during the Reset process.

Cause: When the Reset process takes a long time, a power failure during this process can cause the PLP process to start but not complete correctly if the Reset process finishes afterwards.

Fix: To address this issue, the Reset process is interrupted in cases where it takes a long time and a power failure occurs, allowing the PLP process to be completed correctly.

Severity: High

Likelihood: Low

(29) DRAM controller deadlock

Issue: Host IO may hang during host Rd/Wr operation with VDM (Vendor Defined Message) communication on the PCIe bus. When this condition happens, the drive stops the operation and cannot start the PLP routine causing user-data lost when the drive power gets lost.

Cause: During the Rd/Wr operations, when the VDM message comes in, there is a small timing window to the internal DRAM bus deadlock condition with 3 internal DRAM Wr accesses, due to the DRAM access arbiter getting locked up.

Fix: Modify the drive FW to re-allocate the DRAM range for VDM to eliminate the arbiter from being locked when three different DRAM Wr access (one is for VDM) come in simultaneously.

Severity: High

Likelihood: Low

(30) Format NVM (SES=1)

Issue: When executing the Format NVM command with SES=1 and there is a block that fails to erase, a Sanitize fail response is returned.

Cause: This is due to an implementation error caused by a change in the behavior specification of the Sanitize Block Erase, which shares the same internal process.

Fix: In the Format NVM command, even if the erase fails, the response to the HOST will be assumed as successful.

Severity: Low

Likelihood: Low

(31) Basic Management Command

Issue: Temperature Flags of NVMe Basic Management Command Data return incorrect value for Low Thermal Throttling.

Cause: Temperature Flags of NVMe Basic Management Command Data are set only when there is Thermal Throttling due to overheat and not set in other throttling states.

Fix: Corrected the condition to update the Temperature Flag if the throttling state is not Normal.

Severity: Low

Likelihood: Middle

(32) Log page 05h for Lockdown Command

Issue: Lockdown Command will not change Controller Capabilities. However, Controller Capability Change (CCC) value in the LogPage-0x05 for Lockdown command is reported as 1, which means the command may change the controller capability. It is wrong reporting.

Cause: The CCC value for Lockdown command in LogPage-0x05 has been incorrectly reported as 1 instead of 0.

Fix: Corrected the CCC value of Lockdown command in LogPage-0x05 to 0.

Severity: Low

Likelihood: High

(33) Drive Self Test

Issue: In LBA Format with the use of Meta data and MSET=0, an inappropriate Memory Write occurs to the host's memory during the execution of Drive Self Test (DST) MediaCheck. If the Compare command was executed prior, the Meta data pointer at the time of that command execution is used as an host address. If the Compare command was not executed, address 0 is used.

Cause: In LBA Format using Meta data with MSET=0, when User data Read is performed during DST MediaCheck, the Meta data portion was not properly discarded as it should have been. As a result, the Meta data portion was inappropriately written into the Host Memory area allocated for storing Meta data in previous commands such as Compare.

Fix: Modify the DST MediaCheck processing to properly discard the Meta data as well.

Severity: High

Likelihood: Middle

(34) FW activation hang

Issue: When activating a firmware in the SMBus Reset Assert state, the FW hangs.

Cause: During the firmware activation process, there was an access to the SMBus module registers even when the SMBus Reset Assert was active.

Fix: The process to stop the SMBus module during firmware activation has been modified to ensure that there is no access to the SMBus module registers when the SMBus Reset Assert is active.

Severity: Middle

Likelihood: Middle

(35) VPD Read/Write command

Issue: When VPD Read is aborted by NSSR, then the next VPD Read/Write Commands does not respond correctly.

Cause: NSSR Abort process does not handle the EEPROM module access correctly.

Fix: The drive FW is fixed to handle the EEPROM module access correctly.

Severity: Low

Likelihood: Middle

(36) PCIe data parity Mismatch

Issue: The Data Parity Mismatch bit is inappropriately set during the linkup process.

Cause: After the linkup interrupt, when transitioning from Recovery. Idle to L0 at the initial Link speed of Gen4 and Gen5, the following Data Parity Mismatch bit in Physical Layer 16.0GT/s Extended Cap is being set inappropriately.

Fix: Clear the following Data Parity Mismatch bit in Physical Layer 16.0GT/s Extended Cap during the initial Recovery. Idle to L0 transition after the linkup interrupt for Link speeds of Gen4 and Gen5. Do not clear it for subsequent Recovery. Idle to L0 transitions.

Severity: Low

Likelihood: High

(37) TCG range lock

Issue: When the TCG range lock is enabled, it was possible to induce a failure state in the Drive using the error injection feature.

Cause: NA

Fix: When the TCG range lock is enabled, modify the error injection feature to respond with an error (Operation Denied) when attempting to induce a failure state in the Drive.

Severity: Low

Likelihood: High

(38) CMB (BAR4)

Issue: When CMB (Controller Memory Buffer) is enabled and hot plugged to Host, the drive may not be recognized.

Cause: PCIe BAR4 used for CMB is not Prefetchable attribute right now, so it may not be recognized by Host side.

Fix: Set PCIe BAR4 used for CMB with Prefetchable attribute to be able to be recognized at the time of hot plug-in.

Severity: High

Likelihood: Middle

(39) Reset during I/O and Drive Self Test (DST)

Issue: When executing a Reset during the execution of I/O and Drive Self Test (DST) Extended, the completion time for the I/O abort may exceed 1 second, which could result in a timeout at the host.

Cause: When a reset occurs during I/O execution, the I/O abort process is triggered. However, if the DST extended is running at that time, the DST process may take priority, which can delay the I/O abort process.

Fix: During the I/O command abort process initiated by a reset, the DST processing is temporarily suspended to prioritize the abort process.

Severity: Middle

Likelihood: Middle

(40) SMBus

Issue: Drive cannot respond SMBus command.

Cause: FW reads data from ring buffer when stop condition is detected and then update read pointer. When Stop Condition was not detected and a new Start Condition was detected, only the number of bytes received was initialized and the Read Pointer was not updated, causing the Read Pointer to shift.

Fix: Fix the bug that write index of SMBus ring buffer was out of sync.

Severity: High

Likelihood: Middle

(41) Get Log page (C0h)

Issue: Endurance Estimate in the SMART / Health Information Extended Log (LID=C0h) is mistakenly reported in the unit of GB.

Cause: To speed up the response time for the Get Log Page (LID=02h), the execution time of the processes running in the background has been long, which can lead to noticeable latency due to the delayed start of other tasks.

Fix: The Endurance Estimate field has been corrected to report the value in the unit of bytes.

Severity: Middle

Likelihood: High

(42) PCIe linkup

Issue: There was a delay in the Link-up request from the host until LTSSM Enable, which caused a Polling Active timeout of 24 milliseconds on the host side. In addition to this case, there are instances where the latency of certain processes, such as DSM execution, can be prolonged.

Cause: To speed up the response time for the Get Log Page (LID=02h), background information gathering is being performed; however, the long execution time of this process can result in delays in starting other tasks, leading to increased latency.

Fix: The background task for information gathering has been divided so that other tasks can interrupt and start processing more quickly than before.

Severity: Middle

Likelihood: Low

(43) Command timeout

Issue: Write Zeroes Deallocate command is timed out in case of Verify command is executed repeatedly.

Cause: Interrupt process is executed when Verify NLB (Number of Logical Block) counter is overflowed. There may be a case of missing clearing interrupt status after the process executed. Due to this, in case that the interrupt process is executed repeatedly, CPU is occupied by these interrupts, and subsequent command processing does not proceed, resulting in a command timeout.

Fix: FW is modified to clear the interrupt status correctly when Verify NLB counter is overflowed.

Severity: High

Likelihood: Low

(44) FW Download

Issue: FW activation initiated by NSSR may fail. Also, the NSSR process is aborted at that time and cannot be linked up.

Cause: SMBus interrupts was masked while the FW commit command and SMBus were running, preventing FW from detecting the SMBus command completion interrupt. As a result, the FW Activation process waiting for the SMBus command to complete reached the timeout specified in the Maximum Time for Firmware Activation (MTFA), causing FW activation to fail. Also, when FW activation was triggered by NSSR and failed, the NSSR process could not be restarted.

Fix: FW commit command and SMBus were incorrectly masking SMBus interrupts while SMBus was running. Also, NSSR processing is now restarted when FW Activation initiated by NSSR fails. However, fixing the former problem will not manifest the latter problem.

Severity: Middle

Likelihood: Low

(45) Flush command

Issue: Flush command cannot be executed during Sanitize execution or after Sanitize failed.

Cause: Implementation error.

Fix: Modified FW so that Flush command can be executed Sanitize execution or after Sanitize failed.

Severity: Low

Likelihood: Middle

(46) DRAM (Need power cycle)

Issue: The drive may not become ready after power on.

Cause: The reset de-assert timing to DRAM from SoC was not appropriate.

Fix: The reset de-assert timing to DRAM from SoC was set to the appropriate timing.

Severity: Middle

Likelihood: Low

2. Added features:

(1) Lockdown command

Added lockdown command. Lockdown command is valid to the following commands.

- Firmware Image Download
- Firmware Commit
- Sanitize
- Format NVM
- Security Send/Receive
- SetFeature(FID=02h) Power Management
- SetFeature(FID=0Eh) Timestamp
- VPD Write

(2) Max Payload Size

Issue: CM7 Drive does not take advantage of increased Max Payload Size.

Cause: If the MPS is changed after CSTS.RDY=1, FW will not notice the change, so a trigger is needed to reflect the setting in the Drive's internal settings. Therefore, controller reset is necessary after the MPS is changed.

Fix: Change the firmware behavior, so the availability of Max Payload Size can be triggered by the value update operation.

(3) Telemetry Log

To improve Failure Analysis, parameters of Read/Write commands issued by Host and related internal logs can be retrieved via the Telemetry log. The size of Area 3 of the telemetry log is increased by 2070 blocks (approx. 1036KiB).

DATE OF APPLICATION

This change is applied to the factory line from July 2025.

Prepared by: M.Ikehata

M. Ikehata

Checked by: H.Matsumoto

Hiroki Matsumoto

Approved by: T.Masakawa

Takahiro Masakawa