	HEADERS	DETAILS
1. Intimation of Incident **(T-day, within 1 Hour of the Incident)**	1. Letter / Report Subject -	Reporting of technical glitch
	Name of the Member --	Zerodha Broking Limited
	Member Code -	NSE: 13906; BSE: 6498, MCX: 56550
	2. Designated Officer (Reporting Officer details)	Name: Pankathi H Jain
	3. Date & Time of Incident	06-11-2023; 9:18 AM
	4. Exchanges on which Technical Glitch was encountered (NSE, BSE, MCX, NCDEX, MSEI)	NSE, BSE, MCX
	5. Intimation to clients about the Technical Glitch. (Please attach screenshots of communications to clients)	Bulletin, Tweet, IVR message
	6. Network Connectivity Issues / Hardware Issues / Software Issues / Human Error / Other (Please Specify (if more than one, please separate with commas))	Due to an intermittent issue, some of our users are not able to see executed orders in the orderbook. However, the executed orders are updated on the positions page.
	7. Additional Details about the Technical Glitch, if Any.	The issue was Intermittent. The impact was on the display of orders intermittently. But, the affected orders were displayed to clients on the positions page. The order status was displayed on the positions page correctly for all users. The order placement, order modification and order cancellation were not impacted. The said issue did not affect all users, but only a set of users operating out of a particular Silo (Setup). A bulletin was put up on our website informing clients about the issue. A tweet was also put up. IVR message was played to the clients calling on our support line informing them about the issue.
	1. Date & Time of Incident & Incident duration (in Minutes)	06-11-2023; 9:18 AM; Multiple events with multiple durations which are mentioned below
	2. Incident Description	A set of our clients experienced issues with checking the latest status of their orders and positions while order placement, order modification & order cancellation continued to remain unaffected. The order placement, order modification and order cancellation were not impacted until 10:38 AM. The said issue did not affect all users, but only a set of users operating out of a particular Silo (Setup). Our team is in the process of carrying out an RCA of the issue.

	3. Immediate action taken (provide brief details)	A bulletin was put up on our website informing clients about the issue. A IVR message was put up for incoming calls informing clients about this issue. We also informed our users on Twitter about the same. 09:18 AM: Order and position status updates were affected, but order placement was unaffected. 10:00 AM: The processes that handle streaming order and position updates from our order management system (OMS) slowed down inexplicably. These processes have failovers that mirror them 1:1, but those mirrors also exhibited the same behaviour. We were unable to ascertain the root cause at this point. We deployed an ad-hoc solution to re-sync the slowed down order and position stream data, but the same behaviour caused this to slow down significantly. Order placement was unaffected. 10:38 AM: To bring the slowed streams under control, we stopped order placement for the affected set of users on the silo. 11:22 AM: The orders and positions were synced on Kite, making the updated orders and positions data available to clients. 11:38 AM: After ensuring the stability of the streams, we resumed allowing clients to exit their positions and orders but fresh orders were still blocked. 12:09 PM: All restrictions on order placement are removed.
	4. Business Impact i) Number of Clients Impacted ii) Any other impact	i. We are in process of quantifying the number of clients impacted since the issue involved multiple events. As stated earlier, order placement, order modification and order cancelation were unaffected till 10:38 AM. Of the 1.7 million clients on this particular setup, we received about 8300 calls and 3300 tickets across all segments ii. Further, there was no other impact.
	5. Were alternate trading channles available for clients (list all the alternate channels) i) Was there a spike in traffic on the alternate channels available to clients? If yes, provide details.	Since order placement, order modification and order cancellation were not impacted, there was no need for an alternate trading channel until 10:38 AM. Call and trade desk is available for the impacted users from 10:38 AM till the issue was resolved.
	6. Was the issue caused or encountered by a third-party vendor or service provider? i) Name of the third-party vendor or service provider and a bief description of the issue. ii) Do you have a back-up vendor for the said services	i. We suspect that some changes made at OmneNEST's (our exchange empanelled OMS and RMS vendor) end might have also caused this issue. We have raised a ticket with OmneNEST. RCA from OmneNEST is awaited. ii. We are in the process of building our own RMS and OMS system.
	7. Was the issue encountered on the Exchange-provided environment? If Yes, kindly provide details of initimation and communication sent to the Exchnage.	No
2. Preliminary Incident Report (T+1 day)	8. Did you move operations to the Disaster Recover (DR) site? If, Yes, what was the Recovery Time?	No
	1. Date & Time of Incident & Recovery & Incident duration (in Minutes)	06-11-2023; 9:18 AM; 11:38 AM; Multiple events with multiple durations which are mentioned below

	2. Incident Description & chronology of events (Please provide brief details)	There was an intermittent issue with display of order and position statuses on our trading platform owing to an issue with the position and order streams from the OMS to our application on one of the servers between 9:18 AM till 10:38 AM. However, order placement, order modification and order cancellation were unimpacted. To bring the affected streams under control, we stopped fresh orders from 10:38 AM. Once the correct order and position statuses were updated on our trading platform at 11:22 AM, we allowed users to exit their existing positions from 11:36 AM. Restrictions on order placement were removed at 12:09 PM. The said issue did not affect all users, but only a set of users operating out of a particular Silo (Setup).
	3. Business Impact: Please provide details on the points below: i) Number of clients impacted ii) Number of client orders impacted iii) Any P&L impact iv) Any other impact on Business	i. A section of our clients were impacted by the incident. The number of unique users impacted by this incident were 95.4 k. ii. The number of unique orders impacted by this incident were 112k. iii. No impact on P&L. iv. No other impacts.
	4. Details of Client Complaints Received (Please provide details of claims of impacted clients) i) Number of Complaints Received ii) Number of Complaints Settled iii) Number of pending complaints iv) Total amount claimed by complainants	i. There were few complaints. 5 exchange complaint across all segments as on the date of the submission of this RCA ii. All the client complaints via tickets and calls have been resolved. iii. There are 5 complaint open at the exchange as on date of submission of this RCA. We are actively working on resolving those at the earliest and have submitted our response to the exchange regarding those complaints. iv. The amount claimed by the complainants is approximately Rs. 2.87 lakhs.
	5. Root Cause Summary (Pl attach the detailed Report separately)	After conducting an initial investigation, multiple errors were found on the in-house monitoring dashboard "Grafana". It was found that the position and order streams from the OMS to our application on one of the two servers was impacted, causing the display issue, which lasted till 10:38 AM. At 10:38 AM, the stream on both servers was impacted, and hence orders were stopped. A BoD on both servers helped get the orders and positions data back in sync on both the servers by 11:22 AM. However, errors on Grafana were still incoming, but the order flow and the position flow were unimpacted at this point. Continued investigation revealed that an anti-malware monitoring service called Falcon (proprietary software by CrowdStrike, a listed entity in USA), being used by OmneNEST, was throttling our servers. The Falcon service was stopped on one of the servers. This resulted in the errors on Grafana w.r.t. that server to stop. Further, the Falcon service was stopped on the other server, and at this point, all errors on Grafana stopped. Since these are independent servers functioning independently and the fact that errors stopped in both the servers as soon as Falcon service was stopped leads us to believe that the root cause of the issue was the Falcon service. Further investigation on the Crowdstrike dashboard revealed that the Falcon service license was renewed on Oct 29, 2023. An update was also run automatically on the Falcon service on November 5th, 2023 night. The policy on Falcon was set at "Extra Aggressive" mode, and information on the Crowdstrike forums shows that the Falcon service in "Extra Aggressive" mode has caused degradation issues for the servers on which it is running even in the detection mode. This further, leads us to believe that this was the root cause of the issue. We have since disabled Falcon service across all our OMS servers. Since we have alternative anti-malware detection and prevention services called Cloudflare in place, the disablement of the proprietory Falcon service will not have any impact on the functioning/ monitoring of the OMS servers.
	6. If the issue was caused or encountered by a third-party vendor or service provider, Please provide the below details: i) What services are being provided by the third-party vendor or service provider? ii) Time taken (in Minutes) by third-party vendor or service provider to resolve the issue.	i. Yes, the issue was caused due to a anti malware monitoring service called Falcon being used at OmneNest (an exchange empanelled RMS and OMS vendor). ii. Not Applicable
	7. Has a similar issue been encountered prior to the submission of this RCA Report?	A similar issue hasn't been encountered prior to the submission of this RCA, since Dec 2021 when we started reporting the glitches.

	8. Details of long-term preventive action (please provide all action points for long-term preventive action with the date from which they will be implemented) (please use additional sheets if necessary)	1. We have spread our customers across multiple physically independent data centers, OMS installations, and many leased lines with backup lines. Hence, only a fraction of users will be impacted in such scenarios. 2. We have disabled Falcon service across all our OMS servers. Since we have alternative anti-malware detection and prevention services called Cloudflare in place, the disablement of the proprietory Falcon service will not have any impact on the functioning/ monitoring of the OMS servers. 3. We are actively monitoring the behavior of the Nest OMS system and conducting regular checks to identify any potential anomalies or changes that could impact our system's performance. This proactive approach allows us to address any issues promptly and avoid unexpected disruptions.
3. RCA of Technical Glitch Incident (T + 14 days)	9. Provide a detailed Architecture Diagram of the System.	Attached