

## Incident Reporting Form - RCA

<b>1. Letter/ Report Subject -</b>	Reporting of technical glitch to the exchange
<b>Name of the Member-- Member Code -</b>	Zerodha Broking Limited NSE: 13906, BSE: 6498
<b>2. Designated Officer (Reporting Officer details)</b>	
<b>Name: Venu Madhav</b>	
<b>3. Date &amp; Time of Incident &amp; Incident duration</b>	15-06-2022, 16:21 PM, 38 minutes
<b>4. Incident Description &amp; chronology of events (please use additional sheets)</b>	Annexure 1
<b>5. Business Impact</b>	Annexure 2
<b>6. Immediate action taken (please give full details)(please use additional sheets if necessary)</b>	1. We immediately raised the issue with Cloudflare. 2. We immediately posted a bulletin on our website about the issue.
<b>7. Date &amp; Time of Recovery</b>	15-06-2022, 16:59 PM
<b>8. Root Cause Summary (PI attach the detailed Report separately)</b>	Annexure 3
<b>9. Back up measures available</b>	Cloudflare has many number of automated DRs and redundancies built in, where issues in any area of the network seamlessly migrate to other areas instantly. However, this issue was at the WAF(Web Application Firewall) managed ruleset deployment process level,

	affecting all the DRs across all networks across countries.
<b>10. Details of long-term action (please give full details) (please use additional sheets if necessary)</b>	<p>Cloudflare has confirmed that they have identified improvements to their WAF(Web Application Firewall) managed ruleset deployment process to ensure that</p> <ol style="list-style-type: none"> <li>1. Unnecessary rulesets are not created.</li> <li>2. Rulesets that are referenced by their systems are not deleted.</li> </ol>

**Annexure 1:**

1. Internet Connectivity to our trading platform (along with many other websites) was impacted from 16.21 PM to 16.59 PM owing to what seems to be intermittent connectivity issues via the Cloudflare network for users on certain ISPs.
2. Cloudflare is a vendor that provides CDN, network capacity, and DDoS protection to Zerodha’s public facing internet properties.
3. We have attached the RCA obtained from Cloudflare which confirms that their service was impacted.
4. We have also attached the screenshot showing the status posted by Cloudflare about the outage which confirms that they observed Internet connectivity issues. (Sent as a part of the Intimation mail also).

**Annexure 2:**

There was an intermittent issue with the display of Orders, holdings & positions temporarily on Kite for some of our users.

1. By the time the issue happened the equity market was closed.
2. The issue was Intermittent.
3. The reason behind reporting this is due to the fact that the currency market was open.
4. Only a fraction of the users who were trading currency were intermittently impacted.
5. For those users who were impacted Call and trade desk was open.
6. There were very few complaints and customers were informed to use alternative ISP or use the call and trade route.
7. The users were able to reach our website post multiple retries even when the issue was ongoing.

### **Annexure 3:**

1. The final RCA (attached) received from Cloudflare (CDN vendor) confirms that
  - a. The internet connectivity to our trading platform was impacted as a result of a problem at Cloudflare's end.
  - b. A bug in their internal WAF-managed ruleset deployment process resulted in old ruleset being referenced when not needed. Specifically, several identical replicas of the several Cloudflare Managed Rulesets existed in their systems.
  - c. Purging of unnecessary versions to perform database cleanup resulted in increased error logging in their internal systems which triggered the incident.
  - d. The incident was not identified immediately as error rates and latency did not increase suddenly, but rather, ramped up over time and did not impact all locations equally.