Incident Postmortem: DDoS Attack

## **Summary**

Between times 03:16 and 03:21 ETC, about 500 HTTP POST requests arrived from a set of foreign devices to the NBN Team’s external network.

## **Impact**

The NBN team’s services were severely impacted due to the traffic overloading the network. The flooding caused by the packets affected the daily operations.

## **Detection**

The firewall logs recorded the packet inflow and the incident was discovered through the same.

## **Root Cause**

The vulnerability in Spring 5.3.0 was exploited by a carefully crafted exploit, making use of the headers and data to send the malicious packets.

## **Resolution**

The firewall rules were updated to handle the cases when malicious packets were received. The requests were blocked when the headers and data matched the patterns in the rule.

## **Action Items**

The vulnerability in Spring 5.3.0 was studied in detail, and the packets captured were analysed to find attack patterns. Using these, future attempts were prevented.