Incident Postmortem: Spring4shell Remote code execution

## **Summary**

This was attack based of spring4shell vulnerability where the remote code execution takes place through /tomcatwar.jsp file and affected nbn services and network services and was detected at timestamp 2022-03-20T03:21:00Z.

## **Impact**

It impacted nbn services critically and networks on high level .

## **Detection**

It was detected by searching for spring framework version less than 5.3.x which where less than 5.5.18+.

## **Root Cause**

Spring frameworks and modules where not updated .

## **Resolution**

Systematic update of older spring framework version to newer version.

## **Action Items**

Blocking request through /tomcatwar.jsp and http headers request and systematic updates older spring framework to newer version