Incident Postmortem: Malware Attack on Spring Framework vulnerability

## **Summary**

An attacker was able to compromise the Spring Framework on our nbn services using zero-day vulnerability (Spring4Shell). The attack appears to have been targeted at our external facing infrastructure using Spring Framework 5.3.0

## **Impact**

Downtime across our nbn network leading to impaired service functionality.

## **Detection**

## At 2022-03-20 03:16:34 UTC, Telstra Security Operations detected a malware attack on nbn services using a zero-day vulnerability affecting the Spring Framework

## **Root Cause**

zero-day vulnerability (Spring4Shell)

## **Resolution**

## Firewall rules were implemented to mitigate the attack

## **Action Items**

Firewall rules were implemented and users of affected versions should apply the following mitigation: 5.3.x users should upgrade to 5.3.18+, 5.2.x users should upgrade to 5.2.20+. No other steps are necessary.