Incident Postmortem: Malware attack leading to nbn outage

## **Summary**

**Incident start time:** 2022-03-20T03:16:34Z

**Incident end time:** 2022-03-20T03:21:00Z

**Participants:** Telstra Security Operations, nbn team, Networks team

**Status:** Resolved

**Severity:** 1 - Critical

**Detection Time:** 2022-03-20T03:16:34Z

**Root Cause Fixed Time:** 2022-03-20T05:16:34Z

## **Impact**

1) Downtime of 2 hours of critical infrastructure ‘NBN Connection’ (nbn.external.network).

2) Remote code execution on nbn service infrastructure

## **Detection**

## The firewall logs generated alerts at [ 2022-03-20T03:16:34Z ] for abnormal activity and downtime on nbn services through customer complaints

## **Root Cause**

Zero day vulnerability in Spring Framework 5.3.0 (Spring4Shell), attacking the externally exposed Spring Framework hosted by the nbn services team.

At 2022-03-20T03:16:34Z, an attacker began using a malicious payload to perform remote code execution on the nbn network address “nbn.external.network” using HTTP POST requests with malicious query data on the path “/tomcatwar.jsp”.

## **Resolution**

1. The NBN team was notified of the triaged incident while further investigation and mitigation steps regarding upgrading were communicated soon after the detection.
2. Malicious requests were analyzed to look for patterns.
3. The NBN team was recommended to add firewall rule to block the traffic after identifying the pattern in the malicious requests containing payload from disclodef POC https://github.com/craig/SpringCore0day/blob/main/exp.py

## **Action Items**

1) Adding of firewall rules to block the malicious requests on the Spring Framework.

2) Ensuring updated versions of infratructure systems including the server operating system and the frameworks running on them.

3) Notify threat intelligence to find similar malicious payloads to improve firewall detection

of future attacks