**Incident Postmortem Report: Malware Attack Impacting nbn Services**

**Summary**

**Incident Start:** 2022-03-20T03:16:34Z

**Incident End:** 2022-03-20T05:16:34Z

**Involved Teams:** Telstra Cybersecurity, nbn Services, Network Operations

**Current Status:** Resolved

**Impact Level:** Severity 1 – Critical

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

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

**Incident Impact**

The attack caused significant service degradation and outages across nbn infrastructure. Remote Code Execution (RCE) was successfully carried out on externally hosted systems, resulting in a critical service disruption.

**Detection Overview**

Abnormal traffic patterns were first observed in firewall logs, supported by a surge in customer complaints reporting service interruptions. These combined inputs helped confirm the issue

**Root Cause Analysis**

The source of the incident was traced to the exploitation of a recently discovered zero-day vulnerability — Spring4Shell — targeting a public-facing Spring Framework component managed by the nbn team.

At 03:16:34Z, malicious actors began exploiting the vulnerability by sending HTTP POST requests with encoded commands to the endpoint "/tomcatwar.jsp" hosted on the address nbn.external.network. This enabled remote code execution on the affected infrastructure.

Firewall alerts were triggered during the attack, and subsequent forensic analysis confirmed successful execution of malicious code on the network**.**

**Resolution**

Within the first 30 minutes of detection, Telstra Cybersecurity triaged the issue and escalated it to the nbn team.

Over the next half hour, the Security Operations team conducted a rapid investigation of firewall logs, identified the signature pattern of the attack, and escalated this information to the Network Operations team, who implemented a corresponding firewall block to prevent further exploitation.