From: Telstra Security Operations
To: NBN Team (nbn@email)
Subject: URGENT: Security Incident – Immediate Action Required

Body:

Hello NBN Team,

At **2:16:34 PM AEDT on March 20, 2022**, Telstra Security Operations detected a **malware attack** on **nbn services**, exploiting a **zero-day vulnerability (Spring4Shell - CVE-2022-22965) in the Spring Framework**. This has led to **downtime across our NBN network, impairing service functionality**.

Incident Details:

- **Incident Type:** Remote Code Execution (Spring4Shell - CVE-2022-22965)
- **Affected Systems:** Apache Tomcat servers running **Spring Framework 5.3.0**
- **Severity Level: Critical**
- **Initial Indicators:** Significant spike in **malicious activity** observed in **firewall logs and security dashboard**

Current Mitigation Actions:

- **Blocking identified malicious IPs via firewall rules**
- **Monitoring active attack patterns in logs**
- **Assessing impact on critical services**

Telstra Security Operations is actively monitoring the incident and will provide further updates as the situation evolves. **Please have site reliability engineers on standby for mitigation.**

For reference, please review:

- **Spring Security Advisory - CVE-2022-22965**
- **CISA Cyber Advisory**

For any questions or further coordination, don’t hesitate to reach out.

Kind regards,
Telstra Security Operations