**From:** Telstra Security Operations

**To:** <nbn Team> (<nbn@email>)

**Subject:** ongoing malware attack in NBN connection

—

**Body:**

Hello nbn team,

At <2022-03-20T03:16:34Z> the SOC logs detected an ongoing attack in the services.

Infrastructure name: NBN Connection  
Network hostname: nbn.external.network  
Priority: P1 – Critical

According to the previous investigation, it is caused by a zero day exploit known as Spring4Shell CVE-2022-22965

CVE information:

<https://spring.io/security/cve-2022-22965>

<https://www.cisa.gov/news-events/alerts/2022/04/01/spring-releases-security-updates-addressing-spring4shell-and-spring>

At the moment the service is down, and functionality is impaired due to the malware attack.

For any questions or issues, don’t hesitate to reach out to us.

Kind regards,

Telstra Security Operations