**From:** Telstra Security Operations

**To:** nbn@email

**Subject:** Critical Malware Attack in Spring Framework Based Infrastructure

—

**Body:**

Hello nbn Team,

Alert triggered at : 2022-03-20 T03:16:34Z

The infrastructure : NBN Connection, hostname : nbn.external.network is under a malware attack named "Spring4Shell". The Spring4Shell vulnerability bypasses the patch for [CVE-2010-1622](https://nvd.nist.gov/vuln/detail/CVE-2010-1622), causing CVE-2010-1622 to become exploitable again. We’ve rated the severity to P1 – Critical. Kindly initiate incident response as soon as possible.  
Affected Spring Products and Versions

* Spring Framework
  + 5.3.0 to 5.3.17
  + 5.2.0 to 5.2.19
  + Older, unsupported versions are also affected

Mitigation

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. There are other mitigation steps for applications that cannot upgrade to the above versions. Those are described in the early announcement blog post, listed under the Resources section. Releases that have fixed this issue include:

* Spring Framework
  + 5.3.18+
  + 5.2.20+

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

Kind regards,

Telstra Security Operations