**From:** Telstra Security Operations

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

**Subject:** Urgent - Firewall Rule to Block Spring Framework Vulnerability exploit

**Body:**

Hello nbn Team,

We would like to request the creation of a firewall rule and provide you more information about the ongoing attack.

This vulnerability allows remote attackers to execute arbitrary code on the target system without any authentication.Attackers can achieve this by sending a specially crafted HTTP POST request containing malicious parameters to a application using vulnerable Spring Framework(version 5.3.0 to 5.3.17)

To mitigate this risk, we kindly request creating a firewall rule to block incoming HTTP POST requests containing suspicious parameters targeting the Spring Framework. Specifically, we recommend blocking requests containing any of the following parameters:

* class.module.classLoader.resources.context.parent.pipeline.first.pattern
* Runtime.getRuntime().exec

This vulnerability (CVE-2022-22965) is classified as critical due to its ease of exploitation and potential impact.

Applying the latest security patches to Spring Framework libraries within your applications is crucial to fully address this vulnerability.

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

Kind regards,

Telstra Security Operations