**From**: Telstra Security Operations**To**: NBN Network Team (nbn@email)**Subject**: P1 – Critical Incident: Remote Code Execution (RCE) Vulnerabilities in Spring Framework and Spring Cloud Function (CVE-2022-22963, CVE-2022-22965)****

**Hello NBN Network Team,**

At **[exact incident timestamp]**, we identified a **P1 – Critical** security vulnerability in the Spring Framework, which may be impacting the NBN Network infrastructure. Please see the log snippet below:

* **Client IP**: attacker.ip.address.network1
* **Request Path**: /tomcatwar.jsp
* **Exploit Type**: Remote Code Execution (RCE) via Runtime.exec
* **Timestamp**: [exact incident timestamp]

The attack targeted the /tomcatwar.jsp file via a POST request, with the payload attempting to execute remote code via Runtime.exec.

### **Details of the Vulnerabilities:**

* **CVE-2022-22965** (Spring4Shell):  
  This vulnerability affects Spring Framework versions 5.3.0 to 5.3.17 and 5.2.0 to 5.2.19. It can be exploited under the following conditions:
  + The system is running **JDK 9** or higher.
  + The application uses **Apache Tomcat** as the servlet container.
  + The system is packaged as a **WAR** (Web Application Archive) and uses **spring-webmvc** or **spring-webflux** dependencies.
* **CVE-2022-22963**:  
  This vulnerability affects **Spring Cloud Function** versions and poses similar RCE risks.

### **Vulnerability Context:**

* **CVE-2022-22965** bypasses the patch for **CVE-2010-1622**, reintroducing its exploitability on systems running JDK 9 and later.
* Exploitation of these vulnerabilities can allow attackers to execute arbitrary commands on the system, potentially leading to a full system compromise.

### **Recommended Actions:**

1. **Immediate Updates:**
   * Upgrade to **Spring Framework 5.3.18** or higher if using version 5.3.x.
   * Upgrade to **Spring Framework 5.2.20** or higher if using version 5.2.x.
   * Upgrade to **Spring Cloud Function 3.1.7** or 3.2.3 to address **CVE-2022-22963**.
2. **Patch Management:**
   * Ensure all systems running affected versions of the Spring Framework and Spring Cloud Function are immediately updated.
3. **Vulnerability Scanning:**
   * Run vulnerability scans to identify any other components within the infrastructure that could be impacted by these exploits.
4. **Incident Monitoring:**
   * Enhance monitoring across systems to detect potential exploitation attempts or signs of compromise.
5. **Review Additional Reports:**
   * Review **VMware's Tanzu Vulnerability Report** for **CVE-2022-22965** and **CERT Coordination Center’s Vulnerability Note VU #970766** for further details on the vulnerability.

This is a **P1 – Critical** issue, and immediate action is required to mitigate risks to the NBN Network infrastructure. Your prompt attention to the above-recommended actions is crucial.

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

**Kind regards,**  
Telstra Security Operations