**Incident Postmortem: <Remote code execution attack on Tomcat Web Server> - INCIDENT ID – TELSTRA/S01/01**

## **Summary**

On **2022-03-20** at **03:21 UTC**, an attack was detected by the Telestra Security Operation Team targeting multiple infrastructure services of NBN network. Investigation shows that the exploit attempt is a **remote code execution (RCE) attack** specifically targetting the NBN Connection (nbn.external.network). It was detected targeting one of our Tomcat web servers. The attacker utilized a series of **POST requests** to a JSP endpoint (/tomcatwar.jsp) in an attempt to execute system commands remotely. The attack involved multiple IP addresses and was identified based on suspicious request patterns.

## **Detection**

The incident was discovered through the monitoring of incoming traffic to the web server. **Suspicious POST requests** with payloads containing malicious code were detected. The logs revealed a pattern of **RCE attempt** exploiting a known vulnerability in the Tomcat server configuration, specifically targeting the JSP endpoint. Automated security tools flagged the malicious request patterns.

## **Impact**

The attack had the potential to compromise the **NBN Network’s** **Tomcat web server**, allowing attackers to execute arbitrary commands on the server. The attack could have led to a **security breach**, unauthorized access to sensitive data, and potential service disruption. However, no confirmed data breach or service downtime was observed during the incident.The affected infrastructure is crucial for the company's internet service provision, particularly for high-speed connections.

### **Affected Teams and Notification**

**Affected Infrastructure:**

* **Primary Target:** NBN Connection (nbn.external.network)
  + **Description:** Provides high-speed NBN connection service.
  + **Priority:** P1 – Critical

**Supporting Affected Infrastructure:**

* **Mobile Tower Connection (mobiletower.internal.network)**
  + **Description:** Provides a route between mobile towers across the country for cell service.
  + **Priority:** P2 – High
* **Home & Business Lines (homebiz.internal.network)**
  + **Description:** Provides home & business line products such as VoIP.
  + **Priority:** P2 – High
* **ADSL Connect (adsl.internal.network)**
  + **Description:** Provides ADSL product to customers.
  + **Priority:** P2 – High

### **Impact Assessment**

**Business Impact:**

* **Critical Infrastructure Affected:** The NBN Connection is a critical infrastructure component. The ongoing exploitation may disrupt the availability of high-speed internet services for customers.
* **Secondary Impact:** The Mobile Tower Connection, Home & Business Lines, and ADSL Connect services are also vulnerable, potentially affecting VoIP services and mobile network connectivity.

**Service Disruption:**

* **Primary Disruption:** Service outages are being reported for NBN connections due to exploitation.
* **Secondary Disruption:** Mobile and landline services could experience degradation or outages if the attack spreads further.

## **Root Cause**

The attack exploited an existing vulnerability in the **Tomcat web server** configuration, specifically targeting the **JSP file deployment**. The server was configured to allow certain malicious patterns within the class.module.classLoader.resources.context parameters, which the attacker leveraged to trigger remote command execution.

## **Resolution**

The attack was mitigated by:

* **Blocking the malicious IP addresses** involved in the attack.
* **Deploying security patches** to address the known vulnerability in the Tomcat server.
* **Enhancing server-side input validation** to prevent future injection attempts.
* Conducting a full security audit of the Tomcat web server to ensure there are no lingering threats or misconfigurations.

## **Action Items**

1. **Update and Patch Servers**: Ensure that all Tomcat web servers are up to date with the latest security patches.
2. **Review and Strengthen Configuration**: Implement stricter security configurations on the Tomcat servers, including the removal of unnecessary JSP deployments and more robust input validation mechanisms.
3. **Enhance Monitoring and Logging**: Increase the frequency and scope of security monitoring, particularly for web servers, and ensure that logs are reviewed regularly for suspicious activity.
4. **Incident Response Training**: Conduct a training session for the Web Services and Security teams to improve incident detection and response time.
5. **Post-Incident Review**: Organize a post-incident review meeting to discuss lessons learned and refine security protocols.

This postmortem report serves as a record of the incident and the measures taken to resolve it, with a focus on improving future prevention and response strategies.

### **Lessons Learned**

* **Vulnerability Management:** There was a gap in the patch management process that allowed this exploit to take place. Improved patching protocols and regular vulnerability scans will be implemented to prevent similar attacks in the future.
* **Monitoring and Alerts:** The detection of this attack was reliant on log analysis. Enhanced, real-time monitoring and alert systems will be set up to identify and respond to future threats more quickly.
* **Access Control:** A review of access controls for web applications and servers will be conducted to ensure that unauthorized access is better prevented.