Incident Postmortem:

Spring4Shell Vulnerability Exploit Attempt on NBN Connection Infrastructure

Summary

On March 20, 2022, at 03:16:34 UTC, Telstra Security Operations detected a series of attacks targeting the NBN Connection infrastructure, specifically the nbn.external.network host. The attack attempted to exploit the Spring4Shell vulnerability. The incident was classified as P1 - Critical priority due to the critical nature of the targeted infrastructure. The Security Operations team, Networks team, and NBN team were involved in detecting, analyzing, and mitigating the threat.

Impact

The attack targeted a critical infrastructure component that provides high-speed NBN connection service. While no successful breach was reported, the potential impact could have been severe, possibly disrupting NBN services across the country.

Detection

The incident was detected by Telstra's firewall systems at 2022-03-20T03:16:34Z. The firewall logs showed multiple bypass events with characteristics indicative of a Spring4Shell exploitation attempt.

Root Cause

The root cause of the incident was an attempt to exploit the Spring4Shell vulnerability (CVE-2022-22965) in the Spring Framework. This vulnerability allows attackers to execute arbitrary code on the target system by sending specially crafted HTTP requests.
Specifically, the attackers targeted the "/tomcatwar.jsp" endpoint with POST requests containing payloads attempting to access the classLoader, which is a key characteristic of Spring4Shell exploitation attempts.

Resolution

Upon detection, the following steps were taken to resolve the incident:

1. The Security Operations team immediately notified the NBN team to initiate their incident response protocols.
2. A firewall rule creation request was sent to the Networks team to block the malicious traffic.
3. A firewall rule was implemented to block POST requests to "*.jsp" URLs containing the string "class.module.classLoader" in the request body.

Action Items

Completed:

1. Implemented emergency firewall rule to block Spring4Shell exploitation attempts.
2. Notified relevant teams (Networks and NBN) about the incident.

To be done:

1. Conduct a comprehensive security audit of the NBN Connection infrastructure to identify and patch any vulnerable Spring Framework installations.
2. Update all Spring Framework installations to the latest, patched versions.
3. Implement additional monitoring and alerting for Spring4Shell and similar vulnerabilities.
4. Review and enhance the incident response process to improve reaction time for future incidents.
5. Conduct a lessons learned session with all involved teams to identify areas for improvement in detection, communication, and mitigation strategies.
6. Develop and distribute a security advisory to all relevant teams about the Spring4Shell vulnerability and best practices for prevention.
7. Consider implementing a Web Application Firewall (WAF) with regularly updated rules to provide an additional layer of protection against similar vulnerabilities.
8. Enhance logging and monitoring capabilities to detect and alert on suspicious activities more quickly in the future.