Incident Postmortem: Critical Malware Attack in The Spring Infrastructure

**Summary**

The infrastructure : NBN Connection, hostname : nbn.external.network was 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. This is categorized under RCE attack. Firewall blocking rules can stop the attacks successfully.

**Impact**

**The RCE attack can allow the malicious actors to open a shell in the victim’s system and therefore, get the information from the victims device.**

**Detection**

The brute force in the endpoint /tomcatwar.jsp log capture detected the malware attack. The http header that was vulnerable is

suffix=%>//  
c1=Runtime  
c2=<%  
DNT=1  
Content-Type=application/x-www-form-urlencoded

**Root Cause**

The vulnerable http header, along with the vulnerable endpoint was the root cause of this attack.

**Resolution**

Applied the firewall blockage rule using python. The blocked http header is

suffix=%>//  
c1=Runtime  
c2=<%  
DNT=1  
Content-Type=application/x-www-form-urlencoded

**Action Items**

Mitigated the attack by blocking the vulnerable http header and the vulnerable endpoint.