National Cyber Security Centre

2204011000-NCSC

A part of the **Department of the Environment, Climate & Communications**

NCSC Alert

Critical Vulnerability in Java Spring Framework (CVE-2022-22965, Spring4Shell)
CVSSv3: 9.8 (Critical)

2022-04-01

Status: TLP-WHITE

This document is classified using Traffic Light Protocol. Recipients may share TLP-WHITE *information freely, without restriction. For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.*

Description

The Spring Framework is an application framework and 'inversion of control' container for the Java platform.

Spring has published details of a critical vulnerability that currently exists - **CVE-2022-22965** which impacts **Spring MVC and Spring WebFlux** applications running on **JDK 9+**. The current exploit requires the application to run on Tomcat as a WAR deployment. If the application is deployed as a Spring Boot executable jar, i.e. the default, it is not vulnerable to the current exploit.

However, the nature of the vulnerability is more general and there may be other means of it being exploited. Active scanning and exploitation of this vulnerability has been observed. The NCSC is monitoring for evidence of this activity affecting Irish organisations.

The exploit currently published 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 creates a webshell.

Some researchers have observed this activity with requests such as [1]:

```
GET /stupidRumor\_war/index HTTP/1.1 - Test Request
POST /stupidRumor\_war/index HTTP/1.1 - Exploit Dropping webshell
GET /stupidRumor\_war/tomcatwar.jsp?pwd=j\&cmd=whoami HTTP/1.1 -
Attacker Interaction with Webshell
```

These filenames (tomcatwar.jsp) and parameters are easily changed by attackers.

Spring has released further details regarding this vunerability and the suggested workaround on their blog which can be found at the following link: https://spring.io/blog

Products Affected

If you are using Spring Framework with the following configurations:

- JDK 9 or higher
- Spring MVC and Spring Webflux applications
- Spring Boot executable jars are vulnerable to this CVE but not to the currently published exploit

Impact

Remote Code Execution

[1] https://blog.didierstevens.com/2022/03/31/spring4shell-capture-file/

Recommendations

Spring has released patches for this vulnerability as follows:

- Spring Framework 5.3.18 and 5.2.20, which contain the fixes, has been released
- Spring Boot 2.6.6 and 2.5.12 that depend on Spring Framework 5.3.18 has been released

Workarounds

Applications should extend RequestMappingHandlerAdapter to update the WebDataBinder at the end, after all other initialisation. In order to achieve this, a Spring Boot application can declare a WebMvcRegistrations bean (Spring MVC) or a WebFluxRegistrations bean (Spring WebFlux).

For Spring MVC without Spring Boot, an application can switch from @EnableWebMvc to extending DelegatingWebMvcConfiguration directly as described in Advanced Config section of the documentation, then overriding the createRequestMappingHandlerAdapter method, more details on these workarounds can be found on the Spring Blog Advisory

DISCLAIMER: *This document is provided "as is" without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.*

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@decc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie