

## Spring4Shell Vulnerability

### Public 0-day exploit allows remote code execution

<https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement>  
 CVEs: CVE-2022-22965

A remote code execution vulnerability exists in Spring Framework with JDK version 9 due to an insecure deserialization exploit. The exploit is based on insufficient validation of input that an attacker can perform a remote code execution. Spring is encouraging customers to upgrade to Spring Framework 5.3.18 and 5.2.20 or follow the suggested workarounds.

**Background** Spring Framework is the most popular Java lightweight open-source framework which allows simplification of the software development cycle of any Java-based enterprise applications.

**Announced** March 30, 2022: Spring announced a 0-day vulnerability on their Spring Framework with JDK9.  
 March 30, 2022: A tech news site Cyber Kendra provided vulnerability details and investigation.  
 March 31, 2022: Thousands of SecNews site picked up and re-announced the critical vulnerability.

**Latest Developments** March 31, 2022: Spring published a blog on details, workaround and solution of the vulnerability. FortiGuard is seeing active exploitation of the vulnerability. The telemetrics can be viewed at: <https://www.fortiguard.com/encyclopedia/ips/51352>

## PROTECT

Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:

### Reconnaissance

#### Decoy VM

Detect activities on exploitation of Spring vulnerability (CVE-2022-22965).



**FortiDeceptor**  
DB 20221125


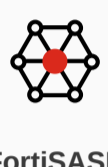


### Weaponization

### Delivery

### Exploitation

#### IPS


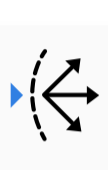
Detect activities on exploitation of Spring vulnerability (CVE-2022-22965).

**FortiGate** DB 20.287    **FortiSASE** DB 20.287    **FortiADC** DB 20.287    **FortiProxy** DB 20.287

#### Web App Security


Detect activities on exploitation of Spring vulnerability (CVE-2022-22965).

**FortiWeb** DB 0.00317    **FortiADC** DB 1.00033

#### Application Firewall

Detect activities on exploitation of Spring vulnerability (CVE-2022-22965).



**FortiClient**  
DB 20.289

### Installation

#### Post-execution

Block post-exploitation activity associated with adversaries attempting to utilize the vulnerability to gain a foothold within the environment.



**FortiEDR**  
v4.0+

### C2




### Action

## DETECT

Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:

#### Threat Hunting


Detect activities on exploitation of Spring vulnerability (CVE-2022-22965).

**FortiDeceptor** v3.0+    **FortiAnalyzer** v7.0    **FortiSIEM** v6.2+

#### Outbreak Detection

Detects indicators for the Spring vulnerability (CVE-2022-22965) across the Security Fabric




**FortiAnalyzer**  
DB 1.052

## RESPOND

Develop containment techniques to mitigate impacts of security events:

#### Automated Response



Services that can automatically respond to this outbreak.



**FortiXDR**

#### Assisted Response Services

Experts to assist you with analysis, containment and response activities.


**Incident Response**    **FortiRecon: ACI**

## RECOVER

Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

#### InfoSec Services

Security readiness and awareness training for SOC teams, InfoSec and general employees.



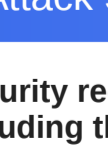
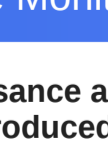
**Response Readiness**

## IDENTIFY

Identify processes and assets that need protection:

#### Attack Surface Monitoring (Inside & Outside)

Security reconnaissance and penetration testing services, covering both internal & external attack vectors, including those introduced internally via software supply chain.

**Security Rating**    **FortiRecon: EASM**

## Additional Resources

- Spring Blog** <https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement>
- FortiGuard Threat Signal** <https://www.fortiguard.com/threat-signal-report/4477>
- National Vulnerability DB** <https://nvd.nist.gov/vuln/detail/CVE-2022-22965>

Learn more about [FortiGuard Outbreak Alerts](#)