Spring4Shell Vulnerability

The Spring Framework team has released a security advisory about a critical vulnerability in Spring versions 5.3.15.RELEASE and 5.2.17.RELEASE. This vulnerability allows remote code execution. Spring is encouraging customers to upgrade to the latest version. For more information, visit [Spring’s official advisory](https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement).

Fortinet Products

- FortiSIEM
- FortiAnalyzer
- FortiSOAR
- FortiDeceptor
- FortiClient
- FortiWeb
- FortiGate
- Fortinet Products

**Product Details**

- **FortiSIEM**
  - Functionality: Web App Security
  - Version: 3.0+
  - Description: Detects indicators for the Spring4Shell vulnerability.
- **FortiAnalyzer**
  - Functionality: IPS
  - Version: 20.287
  - Description: Detects indicators for the Spring4Shell vulnerability.
- **FortiSOAR**
  - Functionality: Outbreak Detection
  - Version: 1.052
  - Description: Compromised server is sniffing over the network looking for a foothold within the environment.
  - Functionality: Post-Execution
  - Version: 20.287
  - Description: Activity associated with adversaries attempting to utilize the vulnerability (CVE-2022-22965).
- **FortiDeceptor**
  - Functionality: Decoy VM
  - Version: 20.289
  - Description: The plays a role in the collapse of MITM attack and helps to detect and mitigate the attack.
- **FortiSOAR**
  - Functionality: Application Firewall
  - Version: 7.0
  - Description: For additional details, read the FortiSOAR update.

**Historical Events**

March 31, 2022: Spring published a blog on details, workaround and solution of the vulnerability.

Thousands of SecNews site picked up and re-announced the critical vulnerability.

FortiGuard is seeing active exploitation of the vulnerability. The telemetrics can be viewed at [FortiGuard](https://www.fortiguard.com/updates/ips?version=20.287).

**More**