



VMware Spring Cloud Function RCE Vulnerability

Critical flaw found in Spring Cloud Function resulting in Remote Code Execution

<https://tanzu.vmware.com/security/cve-2022-22963>
 CVEs: CVE-2022-22963

In Spring Cloud Function versions 3.2.2, 3.1.6, and older versions, it is possible for an attacker to provide a specially crafted malicious expression that may result in remote code execution and access to local resources. With CVSS base score of 9.8 and publicly available proof of concept, this vulnerability should be seriously attended.

Background Spring Framework is an open source lightweight Java-based platform application development framework for creating high-performing, easily testable code. And, Spring Cloud provides developer tools to build distributed systems (e.g. configuration management, service discovery, etc).

In March 2022, another critical vulnerability CVE-2022-22965 known as "Spring4Shell" also affected a flaw in the Spring Framework. See dedicated Outbreak Report for full details:
<https://www.fortiguard.com/outbreak-alert/spring4shell-vulnerability>

Announced March 29, 2022: VMware published a vulnerability report:
<https://tanzu.vmware.com/security/cve-2022-22963>

Latest Developments Dec 20, 2022: FortiGuard Labs is still seeing active attack attempts of the vulnerability CVE-2022-22963 and advises users to upgrade to recommended versions for mitigating the vulnerability.

The FortiGuard telemetry can be viewed at:
<https://www.fortiguard.com/encyclopedia/ips/51355>


PROTECT

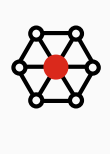
Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:


- Reconnaissance
- Weaponization
- Delivery
- Exploitation


IPS


Detects exploitation of Spring Cloud vulnerability (CVE-2022-22963)


FortiGate
DB 20.309


FortiSASE
DB 20.309



FortiNDR
DB 20.309



FortiADC
DB 20.309


FortiProxy
DB 20.309

Web App Security


Detects exploitation of Spring Cloud vulnerability (CVE-2022-22963)


FortiWeb
DB 0.00318


FortiADC
DB 1.00033

Application Firewall

Detects exploitation of Spring Cloud vulnerability (CVE-2022-22963)



FortiClient
DB 20.309

- Installation
- C2
- Action

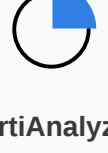
DETECT

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

Outbreak Detection


FortiAnalyzer
DB 1.00081

Threat Hunting

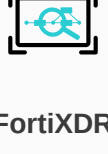

FortiAnalyzer
v6.4+

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


FortiDevSec


FortiDAST

Additional Resources

- VMware** <https://tanzu.vmware.com/security/cve-2022-22963>
- Bleeping Computer** <https://www.bleepingcomputer.com/news/security/springshell-attacks-target-about-one-in-six-vulnerable-orgs/>
- RedHat** <https://access.redhat.com/security/vulnerabilities/RHSB-2022-003>
- Spring4Shell** <https://www.fortiguard.com/outbreak-alert/spring4shell-vulnerability>

Learn more about [FortiGuard Outbreak Alerts](#)