

What is Spring4Shell?

Spring4Shell is the name for CVE-2022-22965, a remote code execution flaw in Spring Framework disclosed on March 31, 2022 with a CVSS score of 9.8. Spring MVC and WebFlux data binding let request parameters set nested object properties, and on JDK 9 or later a parameter path starting with `class.module.classLoader` reached the class loader. On Apache Tomcat with a WAR deployment, attackers used it to reconfigure the access log and write a JSP web shell. Fixed in Spring Framework 5.3.18 and 5.2.20.

HOW IT WORKS

01 How the attack works

Shown for defensive context, the public exploit sent a series of parameters that rewrote Tomcat's access log settings:

- `class.module.classLoader.resources.context.parent.pipeline.first.pattern` set the log line to contain JSP code.
- `...first.directory` and `...first.prefix` pointed the log file into the web root, and `...first.suffix=.jsp` made it executable.
- A follow-up request with a header carrying the JSP fragment was then logged into that file, creating a web shell reachable at a URL like `/shell.jsp?cmd=id`.

Defenders hunting for it looked for `class.module.classLoader` in request parameters and newly created `.jsp` files in Tomcat web roots.

HOW TO DEFEND

- Upgrade Spring Framework to 5.3.18 or 5.2.20 or later (Spring Boot 2.6.6 or 2.5.12 or later pulls them in). Current Spring 6.x lines are not affected.
- Upgrade Tomcat to 10.0.20, 9.0.62 or 8.5.78 or later, which closed the access-log path from the server side.
- Restrict binding. Use `@InitBinder` with `setDisallowedFields` or an allowlist of bindable fields so request parameters cannot reach unexpected properties. That is good practice beyond this CVE.
- Hunt for unexpected JSP files in web roots and `class.module` strings in access logs.

SOURCES

- [1] Spring: CVE-2022-22965 advisory
- [2] NVD: CVE-2022-22965
- [3] CISA Known Exploited Vulnerabilities Catalog
- [4] MITRE ATT&CK: Exploit Public-Facing Application (T1190)

Find the path to a shell before an attacker does.

securelayer7.net/learn/web-exploitation/what-is-spring4shell

[Open online](https://securelayer7.net/learn/web-exploitation/what-is-spring4shell)