Hive Pro

THREAT ADVISORY

RCE Spring Framework Zero-Day vulnerability “Spring4Shell”	TA2022084
Threat Level RED	**Publish Date –** March 31, 2022 **Updated Date –** April 12, 2022

A zero-day vulnerability has been discovered in the Spring framework, a Java framework that provides infrastructure support for web application development. This vulnerability came to light after a Chinese researcher made a GitHub commit that was quickly erased. The vulnerability remained unassigned for over 24 hours before being assigned an official identifier CVE-2022-22965.

The remote code execution bug affects Spring MVC and Spring WebFlux apps running on JDK 9+. By sending a carefully crafted request to a susceptible server, an attacker could exploit Spring4Shell. The publicly available exploit, on the other hand, requires the software to run as a WAR deployment on Tomcat. If the software is deployed as a Spring Boot executable jar, which is the default, it is not vulnerable to this vulnerability. However, the nature of the vulnerability is wide, and there may be many more ways to exploit it.

An active exploitation of Spring4Shell has been observed, an attacker is able to weaponize and execute the Mirai botnet malware on vulnerable servers, specifically in the Singapore region. The Mirai sample is downloaded to the “/tmp” folder and executed after permissions are changed to make them executable using “chmod”

Organizations using Spring Framework with version 5.3.x should upgrade to 5.3.18+ and version 5.2.x should upgrade to 5.2.20+.

Potential MITRE ATT&CK TTPs are:
TA0042: Resource Development
T1588: Obtain Capabilities
T1588.006: Obtain Capabilities: Vulnerabilities
TA0002: Execution
T1203: Exploitation for Client Execution

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name
CVE-2022-22965 (Spring4Shell)	Spring Framework versions 5.3.0 to 5.3.17, 5.2.0 to 5.2.19, and older versions on JDK9+	cpe:2.3:a:vmware:spring_framework:*:*:*:*:*:*:*:*	Spring Framework RCE vulnerability

Indicators of Compromise (IoCs)

Type	Value
SHA-256	69366a4e652041c78c2cc267288a4c4bb0d4eece4074adda82eecd11d9dcf08d, 945d49d58d2d3041aad9445487f01a13d863cf8e76151e9a5008615175f7e52e, 208fc38faf5a2267d837971b48889e855c0edc164c0b2edefff08d0782ccf1bb, 890f25ee7cfb2931536ee3e12fb75ce3f0be21ec03bdfdb38dc688db06e07198, de4040a631b95044e08797837e2143c64ef7c6b981547a9220f8ed7b40701ef9, b73314087130fe98896add3430787744de7310d3342b219bd668cdce79368f91, 596acbbfd7bc54dcc06123b7adfb7337f8ceab736004ce930d8286c8914b8e25, fa7bbc46a7b062a5828380b7c70a67cb47ba10c2ef127fd2348647313f65aa11, 7052cef3936c29707da0dd0d4696863b63971eefa1b0e7db611df2ce26b73f50, 8f429996f5be9d59d86ba4346de535a25b9a2c3e89cf2e29dbc053d13ae99269, ae3fabbbb2e2297e31435b7a57c486f0eaf0f01738da8d0ab68214dc92373666, cf7570cbbca779c755729484792208900a89564669785cb26e88442278ac52b2, 0b63f6e7621421de9968d46de243ef769a343b61597816615222387c45df80ae, 303abc6d8ab41cb00e3e7a2165ecc1e7fb4377ba46a9f4213a05f764567182e5, a0a39c06f56d63b9d37f7e72c24ec0768fe0aff497870ef879d7ae813d84bf1e, 09472d6bfb1c142a3b02f73175254a5e961f91e792dc9b347b099944bcfeab6f, 69366a4e652041c78c2cc267288a4c4bb0d4eece4074adda82eecd11d9dcf08d, 945d49d58d2d3041aad9445487f01a13d863cf8e76151e9a5008615175f7e52e, 208fc38faf5a2267d837971b48889e855c0edc164c0b2edefff08d0782ccf1bb, 890f25ee7cfb2931536ee3e12fb75ce3f0be21ec03bdfdb38dc688db06e07198, de4040a631b95044e08797837e2143c64ef7c6b981547a9220f8ed7b40701ef9, ad03c5f2add8c629f4294b2a7df440cbae213f466e18f98af66db0b82a4e4142, 452a89dd1c760881e0066a5f6c0fc7b5f936a90a197859a4f3ee74b39f705da0, ded51c96d161e9ac22782d7f9df37fe4816eae13be9369f9c8630ee706de53e1, baae0ac6b3873dfdec2587dcddfaf1a327aadf77f7fea6a1532960f31e3dd240
URLs	http://45.95.169.143/The420smokeplace.dns/, http://107.174.133.167/gmpsl, http://107.174.133.167/gi686, http://107.174.133.167/garm, http://107.174.133.167/gmips, http://107.174.133.167/garm7, http://107.174.133.167/gx86, http://107.174.133.167/t.sh, http://107.174.133.167/garm6, http://107.174.133.167/garm5, http://15.185.213.122:65123/javac, http://15.185.213.122:65123, base64://be3f78b59fa14140b6cc8633bf705a75, http://15.185.213.122:65123/java, base64://c08fec5682085417b0a039bdf47c38f2,
MD5	4bcd19351697d04fb357ce5b36600207, 7d244e7bf48d6631b588cecae87e759d, 9c14d670a48bba4b7c047a01d417f8f2, 97a7a357b8290a7236a5fbf45f17569f, 7621f1a5e8db18f3ae30031122c9c397, 100674f1e3ecfb6fa244de4ba7fd2ae2, 329155ab45e244661a7725d81dfad740, 611630a580e33017be32de8c72625489, 650152a2fe78dfceceb4d1a1fdeaccb8,

Indicators of Compromise (IoCs)

Type	Value
MD5	400590515f0f1cf942fe734126be94e7, a8a36132632366c7f65066b23d6f7e4f, b1124c862998bc4ab3ff8b1d471310a6, cca63413e3ca6b834b6a4446768c5ccb, dcc157b2c284ac676000d64dd33f3ec4, e1190f07a6da91caaa317affc9512caa, eba95249cf0a51e300d7b6029cf7088e, fb63e9a23dbf4124116471fcf3254283, fd839753ca4d89c0ccd229b12f95827c
IPV4	46[.]175.146.159:16772, 1[.]85.220.54, 3[.]239.1.141, 5[.]2.69.50, 27[.]102.106.117, 37[.]187.18.212, 43[.]128.201.239, 43[.]242.116.54, 45[.]15.16.105, 45[.]32.251.86, 45[.]128.133.242, 45[.]129.56.200, 46[.]232.251.191, 51[.]77.52.216, 81[.]17.18.59, 85[.]93.218.204, 85[.]204.116.204, 87[.]120.37.231, 91[.]149.225.172, 91[.]211.89.43, 93[.]95.226.212, 94[.]140.114.210, 103[.]140.186.68, 109[.]70.100.19, 142[.]4.206.84, 178[.]17.170.135, 185[.]36.81.95, 185[.]83.214.69, 185[.]100.86.74, 185[.]105.90.134, 185[.]226.67.169, 217[.]138.199.93

Patch Links

https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement
https://tanzu.vmware.com/security/cve-2022-22965

References

https://www.praetorian.com/blog/spring-core-jdk9-rce/
https://www.cyberkendra.com/2022/03/springshell-rce-0-day-vulnerability.html
https://blog.netlab.360.com/what-our-honeypot-sees-just-one-day-after-the-spring4shell-advisory-en/
https://www.trendmicro.com/en_us/research/22/d/cve-2022-22965-analyzing-the-exploitation-of-spring4shell-vulner.html