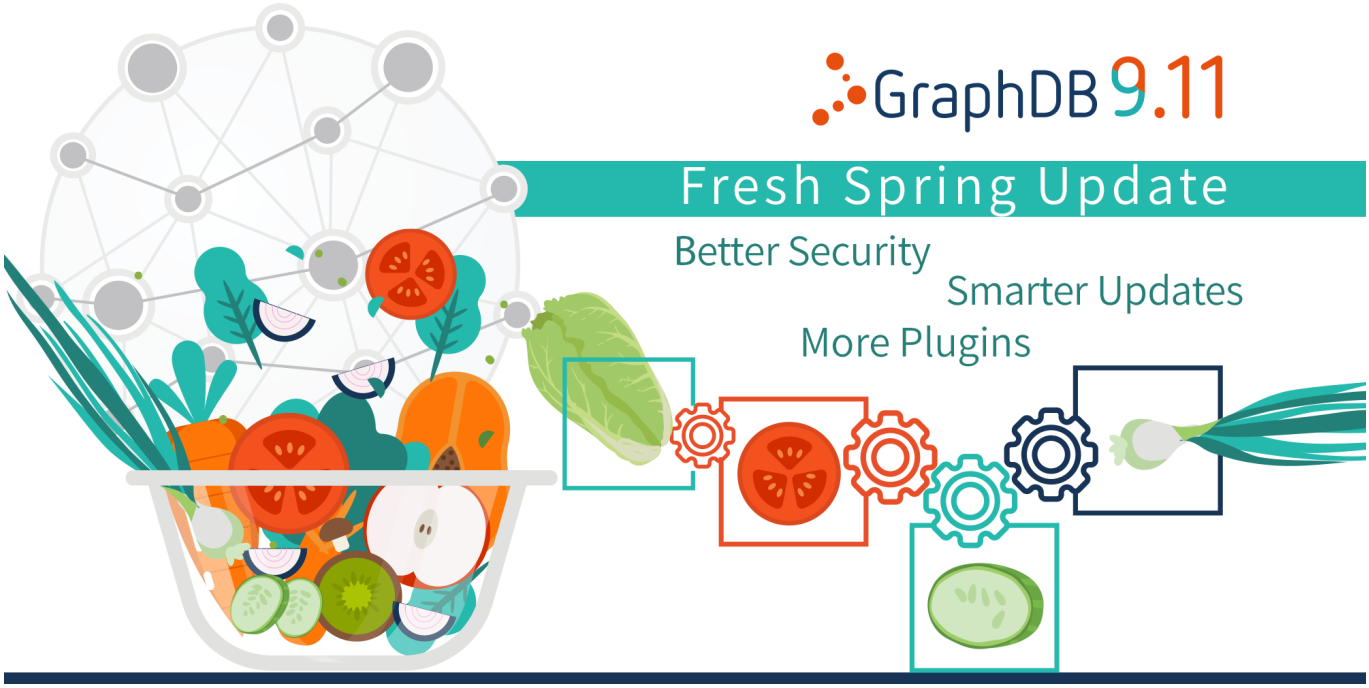
Author: Pavel Mihaylov

ontotext



A zero-day vulnerability is one of the most stressful situations for any operations team, especially when dealing with a vulnerability with the highest severity remote code execution (RCE). The situation is much worse if the vulnerable library (in this case Spring) is in widespread use in thousands of applications.

This is exactly what happened at the end of last week with the announced CVE-2022-22965, also known as Spring4Shell or SpringShell. The vulnerability exposes the class object when binding the parameters in certain types of requests. A public PoC exploit demonstrated RCE using the exposed class loader to modify the Tomcat log configuration and upload a JSP web shell.

What are the preconditions to exploit the vulnerability?

The full extent of the vulnerability is still under revision. From what we know so far, the attacker can exploit it if all of these are met:

Copyright: Ontotext New York | Sofia | Basel
Reach out to us: info@ontotext.com

ontotext

- Running on JDK 9 or higher
- Apache Tomcat as the Servlet container
- Packaged as a traditional WAR and deployed in a standalone Tomcat instance
- spring-webmvc or spring-webflux dependency
- Spring Framework versions 5.3.0 to 5.3.17, 5.2.0 to 5.2.19, and older versions

What is the impact on GraphDB software?

GraphDB uses the Spring framework extensively. In GraphDB 9.9.x, 9.10.x and 9.11.0 the Spring framework is v5.2.15 and as such will be reported as vulnerable by a blind scan that just checks for the existence of certain versions of specific libraries.

We analyzed the vulnerability carefully and we concluded **GraphDB is not vulnerable** due to several independent reasons:

- GraphDB is not packaged as a war file, nor deployed in a standalone Tomcat instance. GraphDB uses a customized embedded Tomcat akin to a Spring Boot executable jar.
- We could not upload a JSP file on GraphDB exploiting the reported vulnerability.
- Even if the JSP file was uploaded, it would not execute as GraphDB was packaged without JSP support.

Since the nature of the vulnerability is more general, and there may be other ways to exploit it, we decided to immediately release GraphDB 9.11.1 with security patches, including two library version upgrades that both address CVE-2022-22965:

- Spring framework upgraded to 5.2.20
- Tomcat upgraded to 9.0.62

Copyright: Ontotext New York | Sofia | Basel
Reach out to us: info@ontotext.com