OneSpan Security Advisory

Vulnerabilities in Java Spring Framework component in OneSpan products

Advisory ID: onespan-sa-20220404-spring4shell

Revision number: 1.2

Date and time of release: April 21 2022 17:00 UTC

Date and time of last update: April 21 2022 17:00 UTC

Summary

Various high-profile vulnerabilities have been identified in the popular Java Spring Framework and related software components. The vulnerabilities are referred to as Spring4Shell.

The following four vulnerabilities have been identified so far:

- Vulnerability CVE-2022-22947 allows performing a remote code execution attack against applications using Spring Cloud Gateway. It affects versions 3.1.0, 3.0.0 to 3.0.6, and older unsupported versions. It is patched in versions 3.1.1 and higher, and 3.0.7 and higher.
- Vulnerability CVE-2022-22950 allows performing a denial-of-service attack against applications using the Spring Framework. It affects versions 5.3.0 to 5.3.16 and older unsupported versions. It is patched in version 5.3.17.
- Vulnerability CVE-2022-22963 allows performing a remote code execution attack against applications using the Spring Cloud Function. It affects versions 3.1.6, 3.2.2 and older unsupported versions. It is patched in versions 3.1.7 and 3.2.3.
- Vulnerability CVE-2022-22965 allows performing a denial-of-service attack against applications using Spring MVC or Spring WebFlux. It affects Spring Framework versions 5.3.0 to 5.3.17, 5.2.0 to 5.2.19, and older unsupported versions. It is patched in versions 5.3.18 and 5.2.20. The vulnerability can only be exploited under certain conditions, i.e. the application has to use JDK 9 or higher, use Apache Tomcat as the Servlet container, and be packaged as a traditional WAR (which is not the default approach).

This security advisory contains information about the security risk that the Spring4Shell vulnerabilities present to OneSpan's SaaS and on-premises products, provides information about compensating measures relevant to on-premises customers, and provides information about the availability of hotfixes.

Risk assessment for OneSpan's products and solutions

1) OneSpan SaaS solutions

OneSpan Sign Production and Sandbox

The vulnerabilities do not apply to OneSpan Sign because it does not use Oracle Java 1.9+. Furthermore OneSpan Sign is equipped with a Web Application Firewall (WAF), which inspects all incoming web traffic. We have configured the WAF to detect and block attempts to exploit Spring4Shell vulnerabilities.

OneSpan Sign FedRAMP environment

The vulnerabilities do not apply to OneSpan Sign FedRAMP because it does not use Oracle Java 1.9+. Furthermore this environment is equipped with Web Application Proxies (WAPs), which perform pre-authentication of most requests to OneSpan Sign.

OneSpan Cloud Authentication (OCA), Intelligent Adaptive Authentication (IAA) and Risk Analytics (RA) based on Trusted Identity (TID) platform

The OCA and IAA solutions do not use a vulnerable version of the Java Spring Framework, and are therefore not impacted by this vulnerability. Furthermore the Staging/Production environments of OCA and IAA are protected with IP-address whitelisting and Transport Layer Security (TLS) with mutual TLS authentication. As such only authenticated customers can access the web applications and APIs of these solutions. Adversaries cannot access the Sandbox environments of OCA and IAA without creating an account in OneSpan's Community Portal.

OneSpan's Identity Verification (IDV) and DealFlo v2 solutions

The vulnerabilities do not apply to the Identity Verifcation and DealFo v2 solutions because they do not use Oracle Java 1.9+. Furthermore the Production environments of IDV and DealFlo v2 are protected with authentication based on Access Tokens. As such, only authenticated customers can access the web applications and APIs of these solutions.

Application Shielding portal

The Application Shielding portal does not use the Java Spring Framework and is therefore not impacted by this vulnerability.

2) OneSpan on-premises server products

Authentication Server Framework

Authentication Server Framework does not use the Java Spring Framework and is therefore not impacted by this vulnerability.

Authentication Server

Authentication Server does not use the Java Spring Framework and is therefore not impacted by this vulnerability.

Authentication Server Appliance

Authentication Server does not use the Java Spring Framework and is therefore not impacted by this vulnerability.

Digipass Gateway

A component of the Digipass Gateway product uses the Java Spring Framework. However Digipass Gateway does not use Oracle Java 1.9+. Therefore Digipass Gateway is not vulnerable.

Risk Analytics

GIS Location Server, a component of Risk Analytics, is vulnerable to CVE-2022-22965 and CVE-2022-22950 if used with JDK 9 or higher. OneSpan has published a hotfix to address the vulnerability.

Digipass Native Bridge

Digipass Native Bridge does not use the Java Spring Framework and is therefore not impacted by this vulnerability.

OneSpan Sign

The vulnerabilities do not apply to OneSpan Sign because it does not use Oracle Java 1.9+.

3) OneSpan Digipass authentication products

OneSpan's mobile authentication products do not use the Java Spring Framework and is therefore not impacted by this vulnerability.

Supplier management

OneSpan is engaging with its suppliers and partners who aid in the delivery and support of its products and solutions in order to understand their exposure to the vulnerabilities and the actions they are taking in order to mitigate the vulnerability, if any.

Product fixes and workarounds

OneSpan has released the following product fixes:

Product	Component	Affected versions	Type of fix
Risk Analytics	GIS Geolocation Server	2.11 – 2.14	Hotfix

Obtaining product releases with fixes

Customers with a maintenance contract can obtain fixed product releases from the Customer Portal. Customers without a maintenance contract should contact their local sales representative.

References

[1] https://tanzu.vmware.com/security/cve-2022-22947
[2] https://tanzu.vmware.com/security/cve-2022-22950
[3] https://spring.io/blog/2022/03/29/cve-report-published-for-spring-cloud-function
[4] https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement

Legal disclaimer