Release Notes for SAS® Business Orchestration Services 10.2, Hot Fix 1

Description	Component	Summary	Test Scenario
A security vulnerability surfaces when you use the Apache Camel Netty component with the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols.	BOSS Core	**Summary:** When you use the Apache Camel Netty component with SSL/TLS, you cannot configure host-name verification. No fix is available in the Netty libraries. To avoid the security issue, the host name and port must be set when you create the SSLEngine. You can set the host name and port in the XML configuration file.	After you apply the hot fix, you can configure host-name verification with SSL/TLS. For configuration information, see the following sections in the *SAS Business Orchestration Services 10.2: User's Guide*: • "Configuring SSL with SAS OnDemand Decision Engine" • "Configuring Camel SSLContextParameters"
The encrypt.sh utility fails.	BOSS Core	**Summary:** With the redesign of SAS Business Orchestration Services to use Spring Boot, a change to the folder structure prevents the encrypt.sh script from finding required JAR files. As a result, the utility does not work.	After you apply the hot fix, the encrypt.sh utility runs successfully.
A security vulnerability exists in Apache ActiveMQ 5.15.13.	Security	**Summary:** In Apache ActiveMQ 5.15.13 and earlier, you can configure the optional ActiveMQ LDAP login module to use anonymous access to the Lightweight Directory Access Protocol (LDAP) server. The anonymous context is used erroneously, which bypasses the password verification altogether.	After you apply the hot fix, the Apache ActiveMQ version is upgraded to 5.15.14 which no longer has this security vulnerability.

Description	Component	Summary	Test Scenario
A security vulnerability exists in Apache Shiro 1.7.	Security	**Summary:** When you use an Apache Shiro version earlier than 1.7.1 with Spring, a specially crafted HTTP request might cause an authentication bypass.	After you apply the hot fix, Apache Shiro is upgraded to version 1.7.1 which no longer has this vulnerability.
A security vulnerability exists in Spring Security.	Security	**Summary:** Spring Security is vulnerable to privilege escalation when it fails to save security context information. An attacker who can use elevated privileges in a small portion of a program can extend those privileges to the entire program by sending maliciously crafted requests to the application.	After you apply the hot fix, Spring Security is upgraded to 2.3.8.RELEASE, which no longer has this security vulnerability.
A security vulnerability exists in Eclipse Jetty 9.4.35.	Security	**Summary:** When Eclipse Jetty 9.4.35 handles a request that contains multiple Accept headers with many quality parameters (for example, **q**), the server might enter a Denial-of-Service (DoS) state due to high CPU use.	After you apply the hot fix, the Eclipse Jetty version is upgraded to version 9.4.39, which no longer has this security vulnerability.