Release Notes for SAS® Fraud Management 6.1_M0, Hot Fix 9

Description	Component	Summary and Business Impact	Test Scenario
You cannot promote rules to production unless you have the Promote Rules Without Review privilege.	RULES STUDIO	**Summary:** A user must be a member of a role that has the Promote Rules Without Review privilege to promote a rule to production. Similarly, a user must be a member of a role that has the Delete Rules Without Review privilege to be allowed to delete a rule from production. By default, the Senior Rules Editor and Rules Administrator roles have these privileges. There should be a separate privilege to allow a user to approve and promote another user's rules to production. **Business Impact:** There is no way to allow a user to approve another user's rule and promote it to production without also giving that user the ability to promote his or her own rules without approval.	After you apply the hot fix, two new privileges exist: • Approve and Promote Rules • Approve and Delete Rules These privileges allow users without the Promote Rules Without Review privilege and Delete Rules Without Review privilege to approve and promote or approve and delete rules edited by another user.
The version of Log4j that is included with SAS Fraud Management contains security vulnerabilities.	SECURITY	**Summary:** The following security vulnerabilities were found for Log4j version 2, which is included in SAS Fraud Management: • CVE-2021-44228 • CVE-2021-44832 **Business Impact:** SAS Fraud Management does not have any known technical or functional dependency on the feature that has the vulnerabilities in Log4j v2.	After you apply the hot fix followed by the SAS Security Updates, the Log4j v2 JAR files are upgraded to version 2.17.1, which is not affected by the vulnerabilities. ***Important***: You must install SAS Security Updates immediately following this hot fix. Refer to the instructions in SAS Note 69006.

Description	Component	Summary and Business Impact	Test Scenario
You cannot remove an unregistered lookup list file from within Rules Studio.	RULES STUDIO	**Summary:** An unregistered lookup list is a lookup list file that exists on the server but is not associated with any active or inactive lookup list. You cannot delete these lookup list files from within Rules Studio. **Business Impact:** Files that are not associated with any lookup list cannot be deleted from the server by using Rules Studio.	After you apply the hot fix, you can remove an unregistered lookup list from the server by using Rules Studio.
You cannot save a lookup list if the combined length of the field names in the list exceeds 4,000 characters.	RULES STUDIO	**Summary:** The combined length of field names for a lookup list cannot be longer than 4,000 characters. **Business Impact:** The number of fields and the length of the field names might cause **Save** operation for a lookup list to fail.	After you apply the hot fix, the combined length of the representation of the lookup list fields is not limited to 4,000 characters. **Note:** Lookup lists are intended for quick hash or key-pair type lookups. For performance reasons, it is recommended that you limit lookup lists to between 20 and 25 columns, including the key column.
The supported version of Google Protobuf-Java contains a security vulnerability.	SECURITY	**Summary:** Google Protobuf-Java 3.14 contains the following security vulnerability: • CVE-2021-22569 **Business Impact:** Google Protobuf-Java is used when custom Python models are installed.	After you apply the hot fix, Google Protobuf-Java 3.19.4 is supported. This version is not affected by the vulnerability.

Description	Component	Summary and Business Impact	Test Scenario
The PostgreSQL JDBC driver version is hardcoded in several files.	ODE TAS DBMS	**Summary:** PostgreSQL can be used for database access within SAS Fraud Management. The version of the Java Database Connectivity (JDBC) driver for PostgreSQL is hardcoded to be 42.2.5 in several files during the installation of SAS Fraud Management. **Business Impact:** If the PostgreSQL JDBC driver version is updated, database connectivity is impacted until several scripts are updated. The following are the impacted areas: • SAS OnDemand Decision Engine • Transaction Analysis Server • Data Services	After you install a new version of the PostgreSQL JDBC driver, follow the instructions in SAS Note 68966.
Cookies without the SameSite Attribute are found.	RULES STUDIO	**Summary:** A security scan finds that a SAS Fraud Management cookie does not have the SameSite attribute. If the SameSite attribute is not set, the default behavior is SameSite=Lax. You must set the value to `Strict` for better prevention of cross-site request forgery. Several SAS® Platform cookies are also missing the SameSite attribute. **Business Impact:** The SameSite attribute on a cookie restricts it to a first-party or same-site context. This restriction helps to prevent cross-site request forgery.	After you apply the hot fix, the SameSite=Strict attribute is added to the `workingBuId` cookie in SAS Fraud Management. The other cookies from SAS Platform can be remediated by following the steps in Configure the Same-Site Cookie Attribute for SAS 9.4M7.