Release Notes for SAS® Fraud Management 6.1_M0, Hot Fix 15

Description	Component	Summary and Business Impact	Test Scenario
In the Common Point of Purchase (CPP) job 6020, the length of the ENT_KEY_RECIPE is hardcoded to 120 characters.	BATCH	**Summary:** In the CPP job 6020, the length of the ENT_KEY_RECIPE parameter is hardcoded to 120 characters. As a result, the ability to customize the list of fields that can be used by CPP for the ENT_KEY_RECIPE is limited. **Business Impact:** You cannot customize the fields used for the ENT_KEY_RECIPE if the sum of the lengths is greater than 120. This limitation reduces the flexibility of CPP.	After you apply the hot fix, the length of the ENT_KEY_RECIPE is set to the sum of the lengths of the fields that comprise the parameter. The field lengths are defined in the Transaction Data Repository (TDR).
Transactions are not sorted correctly on the **Explore** tab.	EXPLORE	**Summary:** The maximum number of transactions displayed on the **Explore** tab should be 99 when a search finds 99 or more transactions. Instead, several transactions are missing from the bottom of the transaction list. When you click a column name to sort the list, a different set of transactions disappears from the bottom of the list. **Business Impact:** The inconsistent display of transactions when sorting can make it difficult to examine transaction details.	After you apply the hot fix, when a search matches 99 or more transactions, exactly 99 transactions are displayed on the **Explore** tab. When you sort the list, the same 99 transactions remain in the list.
The performance of job 4003 is slow.	BATCH	**Summary:** Job 4003 updates the FCM_RULES_FIRED table. The job queries the Transaction Data Repository (TDR) database based on the date-time stamp value in the CMX_CREATE_TIMESTAMP column. The performance of this query can be slow if there is a large amount of data in the database. **Business Impact:** The query used by the 4003 job is not optimal and can result in slow performance.	After you apply the hot fix, the RQO_PROC_UTC_DATETIME column is included in the database query, resulting in better performance for the 4003 job.

Description	Component	Summary and Business Impact	Test Scenario
A rules editor cannot move rules from Testing to Coding.	RULES STUDIO	**Summary:** A user with the Rules Editor role cannot move a rule from the Testing folder back to the Coding folder. The Rules Editor role contains the Add/Delete/Modify Rules privilege, which should allow a user in this role to perform this action. **Business Impact:** A rules editor cannot move rules as required to adequately test rules.	After you apply the hot fix, a rules editor can move a rule from the Testing folder to the Coding folder.
When you define a custom transaction type, a heading under the **Activity** components is **Master File Updates**.	RULES STUDIO	**Summary:** In SAS® Rules Studio, you can define custom transaction types. When configuring the **Activity** components for a new transaction type, there is a **Master File Updates** heading. The check box to select all components is named **Select All Master File Updates**. **Business Impact:** There is no functional impact. It is a display issue on the web page used to define custom transaction types.	After you apply the hot fix, the heading is renamed to **Main File Updates**. The first check box in the section is renamed to **Select All Main File Updates**.

SAS® OnDemand Decision Engine fails to record a transaction in the Transaction Data Repository (TDR) due to decoding issues during the alert processing step.	ENGINE	**Summary:** SAS OnDemand Decision Engine reports an invalid value in one of the model score fields and will not insert the transaction into the TDR database. This issue occurs during the alert processing step for an entity that already has an alert with a call result that contains resurface criteria that is configured as follows:
		You select the **Alert Resurface When Transaction** check box, and then you select the following:
		• **Alert high watermark score increases by**
		• **Transaction score >**
		Below is an example of the error message in the engine log:
		`WARN POST_SCORE_ACTION_FAILED`
		`cmx_tran_id=********************** smh_acct_type="<acct`
		`type>" smh_activity_type="<activity type>"`
		`smh_rtn_code="12" smh_reason_code="ERRR"`
			After you apply the hot fix, the model score value is decoded, and the transaction is inserted when the alert resurface criteria are set as described in the Summary.

Description	Component	Summary and Business Impact	Test Scenario
		`com.sas.finance.fraud.transaction.field.Field$DecodeException: Invalid Z3. value found in field rrr_score_n:` **Business Impact:** Transactions for entities that have alerts are not stored in the TDR database by SAS OnDemand Decision Engine. Alerts for these transactions might not resurface as configured.	
The `reloadLookupList` command for SAS OnDemand Decision Engine does not complete.	ENGINE	**Summary:** When a problematic rule causes a SAS time-out, SAS OnDemand Decision Engine assumes that the process is spinning or has crashed and will destroy the associated SAS session. An error for the transaction is then reported in the log. If the `reloadLookupList` command is running, the command does not complete. No future `reloadLookupList` command will run until SAS OnDemand Decision Engine is restarted. **Business Impact:** An updated lookup list cannot be loaded, and SAS OnDemand Decision Engine cannot be redeployed. This issue prevents updates to lookup lists and rules from being deployed and might prevent fraudulent transactions from being identified.	After you apply the hot fix, the `reloadLookupList` command completes.
The automation interface allows you to check out and assess a closed alert when the contact value is empty.	ANALYST WORKSTATION	**Summary:** When you use the automation interface, you should not be able to assess an alert when the status is CLOSED. However, if the **CONTACT VALUE** field is empty, the automation interface allows you to assess that closed alert. **Business Impact:** Closed alerts can be checked out and assessed.	After you apply the hot fix, you cannot check out and assess a closed alert.
SAS OnDemand Decision Engine does not start if you change the original column order in a lookup list.	RULES STUDIO	**Summary:** In SAS Rules Studio, you can upload a comma-separated values (CSV) file to replace the contents of a lookup list. If the columns in the CSV file do not match the original order of columns for the lookup list, the upload is successful. However, SAS OnDemand Decision Engine will not start after the upload completes.	After you apply the hot fix, SAS Rules Studio checks the column order before you upload a lookup list. If the order does not match the existing lookup list definition,

Description	Component	Summary and Business Impact	Test Scenario

		The error message in the SAS OnDemand Decision Engine log is as follows:
		`2024-08-27T15:56:48,231 [RMI TCP Connection(7)-10.21.23.176] ERROR OSE redeploy 0.1 failed`
		`com.sas.finance.fraud.engine.client.ConfigurationException: SAS exited, see the SAS log, rc=2`
		Business Impact: You are unable to start SAS OnDemand Decision Engine after uploading a CSV file whose column order does not match the defined lookup list. The ability to score transactions is impacted until a corrected CSV file is uploaded.
			the following error message displayed:
			`Unable to upload file <filename>.csv The list name, column names, and column order must exactly match the deployed list content.`

An exception occurs in SAS OnDemand Decision Engine when a V segment key in a transaction contains Unicode characters.	ENGINE	**Summary:** On Oracle and IBM DB2 systems that are configured for UTF-8 and have database stored procedures enabled, SAS OnDemand Decision Engine reports an error when there are Unicode characters in the V segment keys. If stored procedures are disabled, the error does not occur. To disable stored procedures, update the ose.xml configuration file to set both the **selectStoredProcedureEnabled** and the **updateStoredProcedureEnabled** beans to **false**. **Business Impact:** Transactions that contain Unicode characters in V segment keys might not be inserted into the MEH or TDR when UTF-8 is configured and stored procedures are enabled for SAS OnDemand Decision Engine.	After you apply the hot fix, Unicode characters in V segment keys are handled correctly when stored procedures are enabled for the database.
A remote code execution can occur through Application System Properties.	SECURITY	**Summary:** On the **Preferences** tab, under **System Properties ► Deployment**, there is an editable property named **deployment_script_webapp.** Privileged users can set the property to a Unix command or a shell script and it will execute when a user clicks the **Deploy** button on the **Console** tab.	After you apply the hot fix, the **deployment_script_webapp** property is not used. The property is read-only in the web application. If it is already set to a Unix

Description	Component	Summary and Business Impact	Test Scenario
		Business Impact: This vulnerability, if exploited, allows an arbitrary command to be executed on the web application server.	command, the command will not execute during rule deployment.
Path traversal vulnerabilities exist in the web application.	SECURITY	**Summary:** Path traversal vulnerabilities exist in the web application. **Business Impact:** A path traversal vulnerability allows an attacker to access files and directories outside of the web root folder.	After you apply the hot fix, the path traversal vulnerabilities no longer exist in the web application.
Regular expression injection vulnerabilities are found in the web application.	SECURITY	**Summary:** Regular expression injection vulnerabilities are found in the web application. **Business Impact:** An attacker can exploit a regular expression injection to maliciously modify a regular expression, which can cause unintended results to be matched or can result in a denial-of-service attack.	After you apply the hot fix, the regular expression injection vulnerabilities no longer exist in the web application.
A command injection vulnerability is found in the web application.	SECURITY	**Summary:** A command injection vulnerability is found in the web application. **Business Impact:** A malicious hacker can exploit this vulnerability to execute operating system commands.	After you apply the hot fix, the command execution vulnerability no longer exists in the web application.
There are cross-site scripting vulnerabilities in the web application.	SECURITY	**Summary:** There are cross-site scripting vulnerabilities in the web application. **Business Impact:** A user might unknowingly execute malicious code.	After you apply the hot fix, the cross-site scripting vulnerabilities no longer exist in the web application.

Description	Component	Summary and Business Impact	Test Scenario
There is cleartext transmission of sensitive information in the web application.	SECURITY	**Summary:** There is cleartext transmission of sensitive information in the web application. **Business Impact:** An attacker can read the cleartext information by gaining access to the channel being used for communication.	After you apply the hot fix, cleartext transmission of sensitive information no longer occurs in the web application.
There are open redirect vulnerabilities in the web application.	SECURITY	**Summary:** There are open redirect vulnerabilities in the web application. **Business Impact:** Unsanitized input is used in a URL, which might redirect the user to an unexpected site.	After you apply the hot fix, the open redirect vulnerabilities no longer exist in the web application.
There is improper neutralization of CRLF sequences in HTTP headers in the web application.	SECURITY	**Summary:** There is improper neutralization of CRLF sequences in HTTP headers in the web application. **Business Impact:** Malicious input that contains CRLF might be used to split the HTTP response into two responses. An attacker can control the second response , which might be used for a cross-site scripting or a cache poisoning attack.	After you apply the hot fix, CRLF sequences are neutralized in HTTP headers in the web application.
XML external entity injection vulnerabilities exist in the web application.	SECURITY	**Summary:** XML external entity injection vulnerabilities exist in the web application. **Business Impact:** XML external entity injection might result in an attack leading to the disclosure of confidential data or denial of service.	After you apply the hot fix, the XML external entity injection vulnerabilities no longer exist in the web application.