Release Notes for SAS® Fraud Management 4.4_M1, Hot Fix 10
Version 5, Release 16

Description	Component	Summary and Business Impact	Test Scenario
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.	If you are on SAS® 9.4M5 (TS1M5), after you apply this hot fix, the Log4j v2 JAR files are upgraded to version 2.12.4. This version is not affected by the vulnerabilities. If you are on SAS® 9.4 M6 (TS1M6) and apply this 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***: If you are on SAS 9.4M6, you must install SAS Security Updates immediately following this hot fix. Refer to the instructions in SAS Note 69006.
The X-Frame-Options Header is not set in several pages in SAS Fraud Management.	SECURITY	**Summary:** A security scan reports that the X-Frame-Options header is not set on several pages in SAS Fraud Management. The X-Frame-Options header determines whether site content can be embedded in other websites. **Business Impact:** The X-Frame-Options header helps to stop clickjacking attacks by preventing the site content from being embedded into other websites.	After you apply the hot fix, the X-Frame-Options header is set to SAMEORIGIN for the SAS Fraud Management pages that are identified by the security scan. You can enable additional security by following the instructions in Disable Cross-Frame Scripting.

Description	Component	Summary and Business Impact	Test Scenario
			In Step 3 of the instructions, select the SAMEORIGIN option by uncommenting this line: `<prop key="X-Frame-Options">SAMEORIGIN</prop>`
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.