Release Notes for SAS® Fraud Management 6.1_M0, Hot Fix 2

Description	Component	Summary and Business Impact	Test Scenario
There is a reflective cross-site scripting (XSS) vulnerability in the alert search function.	ANYLSTSWORK	**Summary:** When you search for alerts using the **Demographic Search** function on the **Alerts** tab, the **Name** and **Address** fields are vulnerable to cross-site scripting when you select the **Starts With** option. **Business Impact:** An attacker can inject malicious code, which can then execute in your browser session. It is possible for malicious code to be injected into the JavaScript code for two fields in the Demographic Search dialog. The added code could then be executed in the authenticated user's browser session, placing sensitive data at risk of being compromised.	After you apply the hot fix, the **Name** and **Address** fields in the **Demographic Search** function do not run any JavaScript. As a result, the fields are no longer vulnerable to a cross-site scripting attack.