Release Notes for SAS® Fraud Management 6.1_M0, Hot Fix 3

Description	Component	Summary and Business Impact	Test Scenario
Modifying a business unit enables a cross-site scripting vulnerability.	BROWSER	**Summary:** When you edit a business unit, a cross-site scripting vulnerability exists that can be evident when you use Microsoft Internet Explorer, where all script security is disabled. If an attack string that contains a newline character is inserted into the URL, the input validation is bypassed. **Business Impact:** When a business unit is edited in the Manager's Workbench, a cross-site scripting vulnerability allows an attacker to inject malicious code. Then, malicious code can execute in your browser session and place sensitive data at risk of being compromised.	After you apply the hot fix, editing a business unit no longer enables a cross-site scripting attack.