# CWE Detail – CWE-939

## Description

The product uses a handler for a custom URL scheme, but it does not properly restrict which actors can invoke the handler using the scheme.

## Extended Description

Mobile platforms and other architectures allow the use of custom URL schemes to facilitate communication between applications. In the case of iOS, this is the only method to do inter-application communication. The implementation is at the developer's discretion which may open security flaws in the application. An example could be potentially dangerous functionality such as modifying files through a custom URL scheme.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2013-5725: URL scheme has action replace which requires no user prompt and allows remote attackers to perform undesired actions.

**•** CVE-2013-5726: URL scheme has action follow and favorite which allows remote attackers to force user to perform undesired actions.

## Modes of Introduction

**•** Implementation: REALIZATION: This weakness is caused during implementation of an architectural security tactic.

## Potential Mitigations

**•** Architecture and Design: Utilize a user prompt pop-up to authorize potentially harmful actions such as those modifying data or dealing with sensitive information. When designing functionality of actions in the URL scheme, consider whether the action should be accessible to all mobile applications, or if an allowlist of applications to interface with is appropriate. (Effectiveness: N/A)

## Demonstrative Examples

**•** External Application

**•** A call into native code can then be initiated by passing parameters within the URL: