# CWE Detail – CWE-419

## Description

The product uses a primary channel for administration or restricted functionality, but it does not properly protect the channel.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Related Attack Patterns (CAPEC)

* CAPEC-383

## Attack TTPs

**•** T1056.004: Credential API Hooking (Tactics: collection, credential-access)

## Modes of Introduction

**•** Architecture and Design: OMISSION: This weakness is caused by missing a security tactic during the architecture and design phase.

**•** Implementation: N/A

## Common Consequences

**•** Impact: Gain Privileges or Assume Identity, Bypass Protection Mechanism — Notes:

## Potential Mitigations

**•** Architecture and Design: Do not expose administrative functionnality on the user UI. (Effectiveness: N/A)

**•** Architecture and Design: Protect the administrative/restricted functionality with a strong authentication mechanism. (Effectiveness: N/A)

## Applicable Platforms

**•** None (Class: Not Language-Specific, Prevalence: Undetermined)