# CWE Detail – CWE-940

## Description

The product establishes a communication channel to handle an incoming request that has been initiated by an actor, but it does not properly verify that the request is coming from the expected origin.

## Extended Description

When an attacker can successfully establish a communication channel from an untrusted origin, the attacker may be able to gain privileges and access unexpected functionality.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2000-1218: DNS server can accept DNS updates from hosts that it did not query, leading to cache poisoning

**•** CVE-2005-0877: DNS server can accept DNS updates from hosts that it did not query, leading to cache poisoning

**•** CVE-2001-1452: DNS server caches glue records received from non-delegated name servers

## Related Attack Patterns (CAPEC)

* CAPEC-500
* CAPEC-594
* CAPEC-595
* CAPEC-596

## Modes of Introduction

**•** Architecture and Design: N/A

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

## Common Consequences

**•** Impact: Gain Privileges or Assume Identity, Varies by Context — Notes: An attacker can access any functionality that is inadvertently accessible to the source.

## Potential Mitigations

**•** Architecture and Design: Use a mechanism that can validate the identity of the source, such as a certificate, and validate the integrity of data to ensure that it cannot be modified in transit using an Adversary-in-the-Middle (AITM) attack. 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)

## Applicable Platforms

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

## Demonstrative Examples

**•** This application does not check the origin of the intent, thus allowing any malicious application to remove a user. Always check the origin of an intent, or create an allowlist of trusted applications using the manifest.xml file.

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

## Notes

**•** Relationship: While many access control issues involve authenticating the user, this weakness is more about authenticating the actual source of the communication channel itself; there might not be any "user" in such cases.