# CWE Detail – CWE-441

## Description

The product receives a request, message, or directive from an upstream component, but the product does not sufficiently preserve the original source of the request before forwarding the request to an external actor that is outside of the product's control sphere. This causes the product to appear to be the source of the request, leading it to act as a proxy or other intermediary between the upstream component and the external actor.

## Extended Description

If an attacker cannot directly contact a target, but the product has access to the target, then the attacker can send a request to the product and have it be forwarded to the target. The request would appear to be coming from the product's system, not the attacker's system. As a result, the attacker can bypass access controls (such as firewalls) or hide the source of malicious requests, since the requests would not be coming directly from the attacker. Since proxy functionality and message-forwarding often serve a legitimate purpose, this issue only becomes a vulnerability when: The product runs with different privileges or on a different system, or otherwise has different levels of access than the upstream component; The attacker is prevented from making the request directly to the target; and The attacker can create a request that the proxy does not explicitly intend to be forwarded on the behalf of the requester. Such a request might point to an unexpected hostname, port number, hardware IP, or service. Or, the request might be sent to an allowed service, but the request could contain disallowed directives, commands, or resources.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Observed Examples (CVEs)

**•** CVE-1999-0017: FTP bounce attack. The design of the protocol allows an attacker to modify the PORT command to cause the FTP server to connect to other machines besides the attacker's.

**•** CVE-1999-0168: RPC portmapper could redirect service requests from an attacker to another entity, which thinks the requests came from the portmapper.

**•** CVE-2005-0315: FTP server does not ensure that the IP address in a PORT command is the same as the FTP user's session, allowing port scanning by proxy.

**•** CVE-2002-1484: Web server allows attackers to request a URL from another server, including other ports, which allows proxied scanning.

**•** CVE-2004-2061: CGI script accepts and retrieves incoming URLs.

**•** CVE-2001-1484: Bounce attack allows access to TFTP from trusted side.

**•** CVE-2010-1637: Web-based mail program allows internal network scanning using a modified POP3 port number.

**•** CVE-2009-0037: URL-downloading library automatically follows redirects to file:// and scp:// URLs

## Related Attack Patterns (CAPEC)

* CAPEC-219
* CAPEC-465

## Attack TTPs

**•** T1090.001: Internal Proxy (Tactics: command-and-control)

## Modes of Introduction

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

## Common Consequences

**•** Impact: Gain Privileges or Assume Identity, Hide Activities, Execute Unauthorized Code or Commands — Notes:

## Potential Mitigations

**•** Architecture and Design: Enforce the use of strong mutual authentication mechanism between the two parties. (Effectiveness: N/A)

**•** Architecture and Design: Whenever a product is an intermediary or proxy for
 transactions between two other components, the proxy core
 should not drop the identity of the initiator of the
 transaction. The immutability of the identity of the
 initiator must be maintained and should be forwarded all the
 way to the target. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** The weakness here is that the intermediary or the
 proxy agent did not ensure the immutability of the
 identity of the microcontroller initiating the
 transaction.

## Notes

**•** Relationship: This weakness has a chaining relationship with CWE-668 (Exposure of Resource to Wrong Sphere) because the proxy effectively provides the attacker with access to the target's resources that the attacker cannot directly obtain.

**•** Maintenance: This could possibly be considered as an emergent resource.

**•** Theoretical: It could be argued that the "confused deputy" is a fundamental aspect of most vulnerabilities that require an active attacker. Even for common implementation issues such as buffer overflows, SQL injection, OS command injection, and path traversal, the vulnerable program already has the authorization to run code or access files. The vulnerability arises when the attacker causes the program to run unexpected code or access unexpected files.