# CWE Detail – CWE-350

## Description

The product performs reverse DNS resolution on an IP address to obtain the hostname and make a security decision, but it does not properly ensure that the IP address is truly associated with the hostname.

## Extended Description

Since DNS names can be easily spoofed or misreported, and it may be difficult for the product to detect if a trusted DNS server has been compromised, DNS names do not constitute a valid authentication mechanism. When the product performs a reverse DNS resolution for an IP address, if an attacker controls the DNS server for that IP address, then the attacker can cause the server to return an arbitrary hostname. As a result, the attacker may be able to bypass authentication, cause the wrong hostname to be recorded in log files to hide activities, or perform other attacks. Attackers can spoof DNS names by either (1) compromising a DNS server and modifying its records (sometimes called DNS cache poisoning), or (2) having legitimate control over a DNS server associated with their IP address.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2001-1488: Does not do double-reverse lookup to prevent DNS spoofing.

**•** CVE-2001-1500: Does not verify reverse-resolved hostnames in DNS.

**•** CVE-2000-1221: Authentication bypass using spoofed reverse-resolved DNS hostnames.

**•** CVE-2002-0804: Authentication bypass using spoofed reverse-resolved DNS hostnames.

**•** CVE-2001-1155: Filter does not properly check the result of a reverse DNS lookup, which could allow remote attackers to bypass intended access restrictions via DNS spoofing.

**•** CVE-2004-0892: Reverse DNS lookup used to spoof trusted content in intermediary.

**•** CVE-2003-0981: Product records the reverse DNS name of a visitor in the logs, allowing spoofing and resultant XSS.

## Related Attack Patterns (CAPEC)

* CAPEC-142
* CAPEC-275
* CAPEC-73
* CAPEC-89

## Attack TTPs

**•** T1584.002: DNS Server (Tactics: resource-development)

## Modes of Introduction

**•** Architecture and Design: N/A

## Common Consequences

**•** Impact: Gain Privileges or Assume Identity, Bypass Protection Mechanism — Notes: Malicious users can fake authentication information by providing false DNS information.

## Potential Mitigations

**•** Architecture and Design: Use other means of identity verification that cannot be simply spoofed. Possibilities include a username/password or certificate. (Effectiveness: N/A)

**•** Implementation: Perform proper forward and reverse DNS lookups to detect DNS spoofing. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** IP addresses are more reliable than DNS names, but they can also be spoofed. Attackers can easily forge the source IP address of the packets they send, but response packets will return to the forged IP address. To see the response packets, the attacker has to sniff the traffic between the victim machine and the forged IP address. In order to accomplish the required sniffing, attackers typically attempt to locate themselves on the same subnet as the victim machine. Attackers may be able to circumvent this requirement by using source routing, but source routing is disabled across much of the Internet today. In summary, IP address verification can be a useful part of an authentication scheme, but it should not be the single factor required for authentication.

**•** These examples check if a request is from a trusted host before responding to a request, but the code only verifies the hostname as stored in the request packet. An attacker can spoof the hostname, thus impersonating a trusted client.

## Notes

**•** Maintenance: CWE-350, CWE-247, and CWE-292 were merged into CWE-350 in CWE 2.5. CWE-247 was originally derived from Seven Pernicious Kingdoms, CWE-350 from PLOVER, and CWE-292 from CLASP. All taxonomies focused closely on the use of reverse DNS for authentication of incoming requests.