

# [UNIX] Vulnerability in Requests Control of BIND Versions 4 and 8 Allows DNS Spoofing

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-11/0095.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 11/27/02

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 27 Nov 2002 01:11:39 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

Beyond Security would like to welcome Tiscali World Online to our service provider team.

For more info on their service offering IP-Secure, please visit [http://www.worldonline.co.za/services/work\\_ip.asp](http://www.worldonline.co.za/services/work_ip.asp)

-----

Vulnerability in Requests Control of BIND Versions 4 and 8 Allows DNS Spoofing

---

## SUMMARY

CAIS/RNP (the Brazilian Research Network CSIRT) and Vagner Sacramento from DIMAp/UFRN (Department of Computer Science and Applied Mathematics/Federal University of Rio Grande do Norte) made some experiments with several versions of the Internet Software Consortium's (ISC) Berkeley Internet Name Domain (BIND), demonstrating the possibility of successful DNS Spoofing attacks to versions 4 and 8.

The BIND application is one implementation of the Domain Name System (DNS) protocol, maintained by ISC. This application resolves Internet host names into IP addresses and IP addresses back into host names, receiving requests from DNS clients at port fifty-three (53).

The identified vulnerability seriously affects the operation of Internet basic services because many of them depend on DNS to perform their functionalities.

Most of name servers in the Internet are running BIND. Recent information obtained from Bill Manning of the USC/ISI indicates that more than 60% of the current DNS servers still use vulnerable and old versions of BIND.

## Securiteam: [UNIX] Vulnerability in Requests Control of BIND Versions 4 and 8 Allows DNS Spoofing

The problem described on this advisory certifies BIND versions 4 and 8 do not prevent sending of two or more resolution requests for the same domain name allowing DNS Spoofing attacks with significant probability of success.

### DETAILS

Vulnerable systems:

\* BIND 4.9.11 and priors (4.9.x); 8.2.7 and priors (8.2.x); 8.3.4 and priors (8.3.x);

BIND versions 4 and 8 use procedures that allow a remote DNS Spoofing attack against DNS servers.

The attack goal is to anticipate a reply with false information to the target DNS server, making the server to store in its cache a false IP address for a certain domain name.

To better understand the identified vulnerability, consider the following scenario. When n different DNS clients send simultaneous requests to a target DNS server (running BIND 4 or BIND 8) to resolve the same domain name, the target server will forward the requests received to others DNS servers, starting from root-servers and trying to get replies for each one of the requests.

In this context, the identified vulnerability can be exploited if an attacker sends simultaneously n requests to the target DNS server using in each one a different IP source address and the same domain name. The target DNS server will send all the received requests to others DNS servers in order to resolve them. Since these requests will be processed independently, they will be assigned different identifiers (ID). As a result, this server will be waiting for n replies with different IDs for the resolution of the same domain name. The attacker then sends several replies with different IDs to the target DNS server attempting to guess one of the expected replies ID, thus applying a DNS Spoofing attack.

The success probability in the implementation of DNS Spoofing attack in BIND 4 and BIND 8 is calculated by the equation:  $n\text{-request-sent}/65535$ , where n-request-sent is the number of requests sent simultaneously to the target DNS server.

Impact:

Normal operation of many Internet services depends on the proper operation of DNS servers. Thus, other services could be impacted if this vulnerability is successfully exploited. An attacker can use DNS spoofing mechanisms to apply a denial of service attack (DoS) or masquerade as "trusted" entity.

The attacker can inject false information into a DNS cache mapping a host name to an arbitrary IP address. Some direct consequences of DNS spoofing attacks are:

## Securiteam: [UNIX] Vulnerability in Requests Control of BIND Versions 4 and 8 Allows DNS Spoofing

- . Compromise of applications that depend on DNS service to resolve host names (such as SMTP, HTTP, LDAP, FTP, SSH, etc), generating false information and consequently intercepting, analyzing, or intentionally corrupting sensitive data;
- . Impersonation of websites since the attacker can define for example the address of the site `www.mydomain.br` as being the IP address `1.2.3.4`, redirecting the access to a fake web server instead of to the real one;
- . Attacks based on the exploitation of trust relationship among security systems.

### Solutions:

Upgrade to BIND 9.2.1, available at:

<<http://www.isc.org/products/BIND/bind9.html>>  
<http://www.isc.org/products/BIND/bind9.html>

### Actions Recommended:

Some applicable recommendations regarding the security of DNS servers are:

- . Configure DNS server in order to allow the use of recursion only at stations which belong to its domain;
- . Configure anti-spoofing rules on the firewall or border router
- . Considering the network topology, set up the DNS server into a DMZ (demilitarized zone).

In addition, best practices for secure configuration of DNS server referenced on a recently published document by CERT/CC: "Securing an Internet Name Server" should be considered. This document is available in:

<<http://www.cert.org/archive/pdf/dns.pdf>>  
<http://www.cert.org/archive/pdf/dns.pdf>

## ADDITIONAL INFORMATION

### References:

[1] Internet Software Consortium; <<http://www.isc.org>> <http://www.isc.org>

[2] Securing an Internet Name Server; Cricket Liu;  
<[http://www.linuxsecurity.com/resource\\_files/](http://www.linuxsecurity.com/resource_files/)>  
[http://www.linuxsecurity.com/resource\\_files/](http://www.linuxsecurity.com/resource_files/)

[3] DNS and BIND, 4th Edition; Paul Albitz & Cricket Liu; May 2001  
<<http://www.oreilly.com/catalog/dns4/chapter/ch11.html>>  
<http://www.oreilly.com/catalog/dns4/chapter/ch11.html>

[4] Securing an Internet Name Server; CERT Coordination Center; Allen Householder, Brian King, Ken Silva  
<<http://www.cert.org/archive/pdf/dns.pdf>>  
<http://www.cert.org/archive/pdf/dns.pdf>

Securiteam: [UNIX] Vulnerability in Requests Control of BIND Versions 4 and 8 Allows DNS Spoofing

The information has been provided by <mailto:[vagner@natalnet.br](mailto:vagner@natalnet.br)> Vagner Sacramento.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

[list-unsubscribe@securiteam.com](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto:list-subscribe@securiteam.com)

=====

=====

**DISCLAIMER:**

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.