Vulnerability in sending requests control of ISC BIND versions 4 and 8 allows DNS spoofing

Code :
Subject : Vulnerability in the sending requests control of BIND versions 4 and 8 allows DNS spoofing
Date : Aug 01, 2002
Last revised: Sep 05, 2002
Credits : Vagner Sacramento, DIMAp-UFRN
Systems Affected: 4.9.8 and priors (4.9.x); 8.2.6 and priors (8.2.x); 8.3.3 and priors (8.3.x);

1. Abstract

CAIS/RNP 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.

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.

2. Details

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-request-sent*/65535, where *n-request-sent* is the number of requests sent simultaneously to the target DNS server.

3. 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 succesfully exploited. An attacker can use DNS spoofing mechanisms to apply a denial of service attack (DoS) or masquerade as a "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:servers are:

- 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.

4. Systems Affected

DNS Servers running the following versions of ISC BIND:

- 4.9.8 and prior (4.9.x);
- 8.2.6 and prior (8.2.x);
- 8.3.3 and prior (8.3.x);

5. Solutions

Upgrade to BIND 9.2.1, available in:
http://www.isc.org/products/BIND/bind9.html

6. 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

7. References

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

[2] Securing an Internet Name Server; Cricket Liu;
http://www.linuxsecurity.com/resource_files/server_security/securing_an_internet_name_server.pdf

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

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

8. Acknowledgements

To Vagner Sacramento that discovered the vulnerability described in this advisory during the development of his master thesis in the DIMAp/UFRN under the orientation of Prof. Thais Vasconcelos Batista and Prof. Guido Lemos de Souza Filho.

To Thiago Alves da Silva that provides support during the tests at CAIS.

Previous advisories published by CAIS:
http://www.rnp.br/cais/alertas

CAIS PGP key
http://www.rnp.br/chaves/cais-pgp-key.asc

Contact:
+55 (19) 3787-3300
+55 (19) 3787-3301
cais@cais.rnp.br