

CERT Advisory CA-2002-15 Denial-of-Service Vulnerability in ISC BIND 9

Source: <http://www.derkeiler.com/Mailing-Lists/Cert/2002-06/0000.html>

From: CERT Advisory (cert-advisory@cert.org)

Date: 06/04/02

Date: Tue, 4 Jun 2002 16:39:46 -0400 (EDT)
From: CERT Advisory <cert-advisory@cert.org>
To: cert-advisory@cert.org

-----BEGIN PGP SIGNED MESSAGE-----

CERT Advisory CA-2002-15 Denial-of-Service Vulnerability in ISC BIND 9

Original release date: June 04, 2002

Last revised: --

Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

- * Domain Name System (DNS) servers running ISC BIND 9 prior to 9.2.1
Because the normal operation of most services on the Internet depends on the proper operation of DNS servers, other services could be affected if this vulnerability is exploited.

Overview

A denial-of-service vulnerability exists in version 9 of the Internet Software Consortium's (ISC) Berkeley Internet Name Domain (BIND) server. ISC BIND versions 8 and 4 are not affected. Exploiting this vulnerability will cause the BIND server to shut down.

I. Description

BIND is an implementation of the Domain Name System (DNS) that is maintained by the ISC. A vulnerability exists in version 9 of BIND that allows remote attackers to shut down BIND servers. An attacker can cause the shutdown by sending a specific DNS packet designed to trigger an internal consistency check. However, this vulnerability will not allow an attacker to execute arbitrary code or write data to arbitrary locations in memory.

The internal consistency check that triggers the shutdown occurs when the `rdataset` parameter to the `dns_message_findtype()` function in `message.c` is not `NULL` as expected. The condition causes the code to assert an error message and call `abort()` to shut down the BIND server. It is also possible to accidentally trigger this vulnerability using common queries found in routine operation, especially queries originating from SMTP servers.

A vulnerability note describing this problem can be found at <http://www.kb.cert.org/vuls/id/739123>. This vulnerability note includes a list of vendors that have been contacted about this vulnerability.

This vulnerability is also being referenced as CAN-2002-0400:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0400>

II. Impact

Exploitation of this vulnerability will cause the BIND server to abort and shut down. As a result, the BIND server will not be available unless it is restarted.

III. Solution

Apply a patch from your vendor

The ISC has released BIND version 9.2.1. The CERT/CC recommends that users of BIND 9 apply a patch from their vendor or upgrade to BIND 9.2.1.

Appendix A. – Vendor Information

This appendix contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below, we have not received their comments.

Apple

The version of BIND that ships in Mac OS X and Mac OS X Server does not contain this vulnerability.

BSDI

Wind River Systems, Inc. does not include BIND 9 with any version of BSD/OS.

Caldera

Cert: CERT Advisory CA-2002-15 Denial-of-Service Vulnerability in ISC BIND 9

SCO OpenServer from Caldera does not ship BIND9, and is therefore not vulnerable.

Caldera Open UNIX does ship BIND9, and is vulnerable. We are investigating.

Caldera OpenLinux does not ship BIND9, and is therefore not vulnerable.

Compaq Computer Corporation

HP Alpha Server Products:

HP Tru64 UNIX:

Tru64 UNIX is not vulnerable to this reported problem. HP Tru64 UNIX ships with BIND 8.2.2-p5

TCP/IP for HP OpenVms:

TCP/IP for HP OpenVms is not vulnerable to this reported problem. The current versions of TCP/IP for HP OpenVMS ship BIND 8.2.2-p5

HP NonStop Server:

"HP NonStop Himalaya is not vulnerable to this problem. The 'named' function of Domain Name Server (T6021) which is implemented for HP NonStop Himalaya is based on BIND 4.8. NonStop DNS is the only Himalaya software product that includes 'named'."

Cray

Cray, Inc. is not vulnerable since the BIND distributed with Unicos and Unicos/mk is not based on BIND 9.

Engarde

Guardian Digital does not ship BIND 9 in any versions of EnGarde Secure Linux, therefore we are not vulnerable. All versions were shipped with BIND 8.

F5 Networks, Inc.

F5 Networks' products do not include BIND 9, and are therefore not affected by this vulnerability.

FreeBSD

The FreeBSD base system does not ship with ISC BIND 9. However, ISC BIND 9 is available in the FreeBSD Ports Collection. It is currently at version 9.2.1 and is therefore unaffected.

Hewlett-Packard Company

HP is Vulnerable, Solution investigation continuing..

IBM

Cert: CERT Advisory CA-2002-15 Denial-of-Service Vulnerability in ISC BIND 9

After analysis of the affected component, IBM has determined that the AIX bind daemon is not vulnerable to the attack as described in the CERT advisory.

Internet Software Consortium

This vulnerability was found through routine bug analysis. BIND 9 is designed to exit when it detects an internal consistency error to reduce the impact of bugs in the server. ISC strongly recommends that all BIND 9 users upgrade immediately to 9.2.1. BIND 9.2.1 can be found at <http://www.isc.org/products/BIND/bind9.html>.

MandrakeSoft

Mandrake Linux 8.x ships with BIND9 and as such updated packages will be available as early as possible.

Microsoft Corporation

Microsoft has reviewed the information and can confirm that our products are not affected by this vulnerability.

NEC Corporation

sent on June 3, 2002
[Server Products]
* EWS/UP 48 Series operating system
– is NOT vulnerable.

NetBSD

NetBSD has not included Bind 9 in the base system of any release or –current development branch.

Bind 9 is available from the 3rd party software system, pkgsrc. Users who have installed net/bind9 or net/bind9-current should update to a fixed version. pkgsrc/security/audit-packages can be used to keep up to date with these types of issues.

Network Appliance

All NetApp products do not contain any BIND code, so no NetApp product is vulnerable to this problem.

Nortel Networks Limited

Nortel Networks is reviewing its portfolio to determine if any products are affected by the vulnerability noted in CERT Advisory CA-2002-15. A definitive statement will be issued shortly.

Red Hat

Cert: CERT Advisory CA-2002-15 Denial-of-Service Vulnerability in ISC BIND 9

Red Hat distributed BIND 9 in Red Hat Linux versions 7.1, 7.2, and 7.3. We are currently working on producing errata packages, when complete these will be available along with our advisory at the URL below. At the same time users of the Red Hat Network will be able to update their systems using the 'up2date' tool.

<http://rhn.redhat.com/errata/RHSA-2002-105.html>

Silicon Graphics, Inc.

IRIX does not ship with BIND9 and is not vulnerable.

Sun Microsystems

Sun does not ship BIND 9 with any version of Solaris at this time and is therefore not affected by this issue.

SuSE, Inc.

We are affected by the bind9 DoS issue as well. All of our currently supported SuSE Linux products come with a bind9 package. We will release an announcement for the issue, coordinated with your timeframe and not before we see your official announcement.

Unisphere Networks, Inc.

The Unisphere Networks ERX family of edge routers does not implement a DNS server or named daemon within the Unison OS. Additionally, the DNS client found on the ERX is not based on the ISC BIND code. Unisphere Networks has no reason to expect a similar problem exists in the DNS client implementation found on the ERX.

The CERT Coordination Center thanks the Internet Software Consortium for notifying us about this vulnerability.

Author: Ian A. Finlay

This document is available from:

<http://www.cert.org/advisories/CA-2002-15.html>

CERT/CC Contact Information

Email: cert@cert.org

Phone: +1 412-268-7090 (24-hour hotline)

Fax: +1 412-268-6989

Postal address:

CERT Coordination Center

Software Engineering Institute

Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from http://www.cert.org/CERT_PGP.key

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site <http://www.cert.org/>

To subscribe to the CERT mailing list for advisories and bulletins, send email to majordomo@cert.org. Please include in the body of your message

subscribe cert-advisory

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

NO WARRANTY

Any material furnished by Carnegie Mellon University and the Software Engineering Institute is furnished on an "as is" basis. Carnegie Mellon University makes no warranties of any kind, either expressed or implied as to any matter including, but not limited to, warranty of fitness for a particular purpose or merchantability, exclusivity or results obtained from use of the material. Carnegie Mellon University does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

Conditions for use, disclaimers, and sponsorship information

Copyright 2002 Carnegie Mellon University.

Revision History

June 04, 2002: Initial release

-----BEGIN PGP SIGNATURE-----

Version: PGP 6.5.8

iQCVAwUBPP0kn6CVPMXQI2HJAQFEyQP/fkgF01EWoE2JPDB3kPwLhSUSrM8XHNvQ
+vfuH8ZSUAiG0/g/zSGjeTt0NFYeeI6kMS7MQqS76ECaP9317gR/zucShEkOKliy
4NHjoF34gPqPIDu6BAdh2xf19q+LNdu8EHs8rj11FqjvPKmL436tS0ToJXqXDpmx
/WHO3P3AwhM=
=M/6l

-----END PGP SIGNATURE-----

- *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)