CERT Advisory CA-1999-14 Multiple Vulnerabilities in BIND

Original release date: November 10, 1999
Last revised: April 25, 2000
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Systems running various versions of BIND

I. Description

Six vulnerabilities have been found in BIND, the popular domain name server from the Internet Software Consortium (ISC). One of these vulnerabilities may allow remote intruders to gain privileged access to name servers.

Vulnerability #1: the "nxt bug"

Some versions of BIND fail to properly validate NXT records. This improper validation could allow an intruder to overflow a buffer and execute arbitrary code with the privileges of the name server.

NXT record support was introduced in BIND version 8.2. Prior versions of BIND, including 4.x, are not vulnerable to this problem. The ISC-supplied version of BIND corrected this problem in version 8.2.2.

Vulnerability #2: the "sig bug"

This vulnerability involves a failure to properly validate SIG records, allowing a remote intruder to crash *named*; see the impact section for additional details.

SIG record support is found in multiple versions of BIND, including 4.9.5 through 8.x.

Vulnerability #3: the "so_linger bug"

By intentionally violating the expected protocols for closing a TCP session, remote intruders can cause *named* to pause for periods up to 120 seconds.

Vulnerability #4: the "fdmax bug"

Remote intruders can consume more file descriptors than BIND can properly manage, causing *named* to crash.

Vulnerability #5: the "maxdname bug"

Improper handling of certain data copied from the network could allow a remote intruder to disrupt the normal operation of your name server, possibly including a crash.

Vulnerability #6: the "naptr bug"

Some versions of BIND fail to validate zone information loaded from disk files. In environments with unusual combinations of permissions and protections, this could allow an intruder to crash *named*.

Other recent BIND-related vulnerabilities

AusCERT recently published a report describing denial-of-service attacks against name servers. These attacks are unrelated to the issues described in this advisory. For information on the denial-of-service attacks described by AusCERT, please see AusCERT Alert AL-1999.004 available at:

ftp://ftp.auscert.org.au/pub/auscert/advisory/AL-1999.004.dns_dos

II. Impact

Vulnerability #1

By exploiting this vulnerability, remote intruders can execute arbitrary code with the privileges of the user running *named*, typically root.

Vulnerabilities #2, #4, and #5

By exploiting these vulnerabilities, remote intruders can disrupt the normal operation of your name server, possibly causing a crash.

Vulnerability #3

By periodically exercising this vulnerability, remote intruders can disrupt the ability of your name server to respond to legitimate queries. By intermittently exercising this vulnerability, intruders can seriously degrade the performance of your name server.

Vulnerability #6

Local intruders who gain write access to your zone files can cause *named* to crash.

III. Solution

Apply a patch from your vendor or update to a later version of BIND

Many operating system vendors distribute BIND with their operating system. Depending on your support procedures, arrangements, and contracts, you may wish to obtain BIND from your operating system vendor rather than directly from ISC.

Appendix A contains information provided by vendors for this advisory. We will update the appendix as we receive more information. If you do not see your vendor's name, the CERT/CC did not hear from that vendor. Please contact your vendor directly.

Appendix A. Vendor Information

Vendor Name

Caldera
See ftp://ftp.calderasystems.com/pub/OpenLinux/updates/2.3/current

```
MD5s
        db1dda05dbe0f67c2bd2e5049096b42c  RPMS/bind-8.2.2p3-1.i386.rpm
        82bbe025ac091831904c71c885071db1  RPMS/bind-doc-8.2.2p3-1.i386.rpm
        2f9a30444046af551eafd8e6238a50c6  RPMS/bind-utils-8.2.2p3-1.i386.rpm
        0e4f041549bdd798cb505c82a8911198  SRPMS/bind-8.2.2p3-1.src.rpm
```

Compaq Computer Corporation

At the time of writing this document, Compaq is currently investigating the potential impact to Compaq's BIND release(s).

As further information becomes available Compaq will provide notice of the completion/availability of any necessary patches through AES services (DIA, DSNlink FLASH and posted to the Services WEB page) and be available from your normal Compaq Services Support channel.

Data General

We are investigating. We will provide an update when our investigation is complete.

Hewlett-Packard Company

HP is vulnerable, see the chart in the ISC advisory for details on your installed version of BIND. Our fix strategy is under investigation, watch for updates to this CERT advisory in the CERT archives, or an HP security advisory/bulletin.

IBM Corporation

The bind8 shipped with AIX 4.3.x is vulnerable. We are currently working on the following APARs which will be available soon:

APAR 4.3.x: IY05851
To Order

APARs may be ordered using Electronic Fix Distribution (via FixDist) or from the IBM Support Center. For more information on FixDist, reference URL:

http://aix.software.ibm.com/aix.us/swfixes/

or send e-mail to aixserv@austin.ibm.com with a subject of "FixDist".

IBM and AIX are registered trademarks of International Business Machines Corporation.

The Internet Software Consortium

ISC has published an advisory regarding these problems, available at

http://www.isc.org/products/BIND/bind-security-19991108.html

The ISC advisory also includes a table summarizing which versions of BIND are susceptible to the vulnerabilities described in this advisory.

OpenBSD

As far as we know, we don't ship with any of those vulnerabilities.

Santa Cruz Operation, Inc

Security patches for the following SCO products will be made available at http://www.sco.com/security

OpenServer 5.x.x, UnixWare 7.x.x, UnixWare 2.x.x

Sun Microsystems

Please see updated information at:

Sun Microsystems, Inc. Security Bulletin #00194: BIND

Vulnerability #1

Solaris 2.3, 2.4, 2.5, 2.5.1, 2.6, and 7 are not vulnerable.
Vulnerability #2

Solaris 2.3, 2.4, 2.5, 2.5.1, 2.6, and 7 are not vulnerable.
For Vulnerabilities #3, #4, #5, and #6:

Solaris 2.3, 2.4, 2.5, 2.5.1, and 2.6 are not vulnerable.
Sun has produced the following patches for Solaris 7.

Solaris version	Patch ID
Solaris 7 (SPARC)	107018-02
	106938-03
Solaris 7 (Intel)	107019-02
	106939-03

The CERT Coordination Center would like to thank David Conrad, Paul Vixie and Bob Halley of the Internet Software Consortium for notifying us of these problems and for their help in constructing the advisory, and Olaf Kirch of Caldera for notifying us of some of these problems and providing technical assistance and advice.

Revision History

November 10, 1999: Initial release
April 25, 2000: Updated vendor information for Sun