CERT Advisory CA-1996-02 BIND Version 4.9.3

==========
CERT(sm) Advisory CA-96.02
Original issue date: February 15, 1996
Last revised: August 13, 1997
Superseded by CA-97.22

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

Topic: BIND Version 4.9.3
- ----------

** This advisory has been superseded by CA-97.22.bind **

Vulnerabilities in the Berkeley Internet Name Domain (BIND) program make it possible for intruders to render Domain Name System (DNS) information unreliable. At the beginning of this year, a version of BIND (4.9.3) became available that fixes several security problems that are being exploited by the intruder community.

The CERT staff urges you to install the appropriate patch from your vendor. If a patch is not currently available, an alternative is to install BIND 4.9.3 yourself. (Note: Although BIND will be further improved in the future, we urge you to upgrade now because of the seriousness of the problems addressed by version 4.9.3.) If neither of the above alternatives is possible, we strongly recommend blocking or turning off DNS name-based authentication services such as rlogin.

We will update this advisory as we receive additional information.
Please check advisory files regularly for updates that relate to your site.

- ----------

I. Description

Version 4.9.3 of the Berkeley Internet Name Domain (BIND) program fixes several security problems that are well known and being exploited by the intruder community to render Domain Name System (DNS) information unreliable.

BIND is an implementation of the Domain Name System. (For details, see RFC 1035, a publication of the Internet Engineering Task Force.) The full distribution of BIND includes a number of programs and resolver library routines. The main program is "named", the daemon that provides DNS information from local configuration files and a local cache. The named daemon is often called /etc/named or /etc/in.named. Programs such as Telnet communicate with named via the resolver library routines provided in the BIND distribution.

Services in widespread use that depend on DNS information for authentication include rlogin, rsh (rcp), xhost, and NFS. Sites may have installed locally other services that trust DNS information. In addition, many other services, such as Telnet, FTP, and email, trust DNS information. If these services are used only to make outbound connections or informational logs about the source of connections, the security impact is less severe than for services such as rlogin. Although you might be willing to accept the risks associated with using these services for now, you need to consider the impact that spoofed DNS information may have.

Although the new BIND distributions do address important security problems, not all known problems are fixed. In particular, several problems can be fixed only with the use of cryptographic authentication techniques. Implementing and deploying this solution is non-trivial; work on this task is currently underway within the Internet community.

The CERT staff has received information that the next minor release of BIND nameserver will be enforcing RFC952 (as modified by RFC1123) hostname conformance as part of its SECURITY measures. Following The BIND release, hostnames that fail to conform to these rules will be unreachable from sites running these servers.

Hostnames (A records) are restricted to the following characters only:

"A" - "Z", "a" - "z", "0" - "9", "." and "-"

These characters are specifically excluded: "_" and "/".

For a full description of what is allowed in a hostname, please refer to RFC952 and RFC1123, available from

http://ds.internic.net/ds/

RFC952: DOD INTERNET HOST TABLE SPECIFICATION, October 1985
RFC1123: Requirements for Internet Hosts -- Application and Support, October 1989

A program is available for checking hostnames and IP addresses. It is available in

ftp://info.cert.org/pub/tools/ValidateHostname/IsValid.c
ftp://ftp.cert.dfn.de/pub/tools/net/ValidateHostname/IsValid.c

The following files are in the directory (from the README):

IsValid.l — The lex/flex file containing the code for IsValidHostname and IsValidIPAddress
MD5 (IsValid.l) = 2d35040aacae4fb12906eb1b48957776

IsValid-raw.c — The C file created by running flex on IsValid.l
MD5 (IsValid-raw.c) = 367c77d3ef84bc63a5c23d90eeb69330

IsValid.c — The editted file created by internalizing variable and function definitions in IsValid-raw.c
MD5 (IsValid.c) = ffe45f1256210aeb71691f4f7cdad27f

IsValid.diffs — The set of diffs between IsValid-raw.c and IsValid.c
MD5 (IsValid.diffs) = 3619022cf31d735151f8e8c83cce3744

htest.c — A main routing for testing IsValidHostname and IsValidIPAddress
MD5 (htest.c) = 2d50b2bffb537cc4e637dd1f07a187f4

II. Impact

It is possible for intruders to spoof BIND into providing incorrect name data. Some systems and programs depend on this information for authentication, so it is possible to spoof those systems and gain unauthorized access.

III. Solutions

The preferred solution, described in Section A, is to install your vendor's patch if one is available. An alternative (Section B) is to install the latest version of BIND. In both cases, we encourage you to take the additional precautions described in Section C.

A. Obtain the appropriate patch from your vendor and install it according to instructions included with the program.

Redistributing BIND and all programs affected by these problems is not a simple matter, so some vendors are working on new named daemon as an immediate patch. Although installing a new named daemon addresses some problems, significant problems remain that can be addressed only by fully installing fixes to the library resolver routines.

If your vendor's patch does not include both named and new resolver routines, we recommend that you install the current version of BIND (Solution B) if possible. We also encourage you to take the precautions described in Section C.

Below is a list of the vendors and the status they have provided concerning BIND. More complete information is provided in Appendix A of this advisory. We will update the appendix as we receive more information from vendors.

If your vendor's name is not on the list, contact the vendor directly for status information and further instructions.

Vendor	New named available	Full distribution available
Digital Equipment		Work is under way.
Hewlett-Packard	Under investigation.	Currently porting and testing (BIND 4.9.3) for the Q1, Calendar 97 general release. Patch in process for 10.X releases.
IBM Corporation		Work is under way.

NEC Corporation	Work is under way.
Santa Cruz Operation	Under consideration.
Silicon Graphics, Inc.	Under investigation.
Solbourne (Grumman)	Customers should install BIND 4.9.3.
Sun Microsystems	Patches available.

B. Install the latest version of BIND (version 4.9.3), available from Paul Vixie, the current maintainer of BIND:

ftp://ftp.vix.com/pub/bind/release/4.9.3/bind-4.9.3-REL.tar.gz

MD5 (bind-4.9.3-REL.tar.gz) = da1908b001f8e6dc93fe02589b989ef1

Also get Patch #1 for 4.9.3:

ftp://ftp.vix.com/pub/bind/release/4.9.3/Patch1

MD5 (Patch1) = 5d57ad13381e242cb08b5da0e1e9c5b9

To find the most current version of bind, see
ftp://info.cert.org/pub/latest_sw_versions/

C. Take additional precautions.

To protect against vulnerabilities that have not yet been addressed, and as good security practice in general, filter at a router all name-based authentication services so that you do not rely on DNS information for authentication. This includes the services rlogin, rsh (rcp), xhost, NFS, and any other locally installed services that provide trust based on domain name information.

.....

Appendix A

Below is information we have received from vendors. If you do not see an entry for your vendor, please contact the vendor directly for status information and further instructions.

- ---

Paul Vixie

See Updates Section

- ---

Digital Equipment Corporation

At the time of writing this advisory, Digital intends to support the final revision of BIND 4.9.3. The project plan for incorporating Version 4.9.3 BIND for Digital's ULTRIX platforms has been approved. This includes 4.3, V4.3A, V4.4 and V4.5.

A similar project plan for Digital UNIX versions is under review. The first implementations will be V3.0 through V3.2D, and V4.0, when released. It is our plan to evaluate and then incorporate V4.9.3 Bind into other UNIX versions as necessary to reduce risk to our customer base.

Digital will provide notice of the completion of the kits through AES services (DIA, DSNlink FLASH) and be available from your normal Digital Support channel.

- ---

Hewlett-Packard Company

The named daemon is under investigation. HP will provide updated information for the CERT advisory.

HP is currently porting and testing BIND 4.9.3 for a general release first quarter of 1997. A patch is in process for 10.X releases. Watch for CERT advisory updates and a Security Bulletin from HP.

- ---

IBM Corporation

Work is under way.

- ---

NEC Corporation

Some systems are vulnerable. We are developing the patches and plan to put them on our anonymous FTP server. You can contact us with the following e-mail address if you need.

E-mail: UX48-security-support@nec.co.jp
FTP server: ftp://ftp.meshnet.or.jp

- --
The Santa Cruz Operation, Inc.

SCO is currently considering a port of the new BIND into its product line,
but no timeline is yet available. This includes SCO OpenServer and SCO
UNIXWare.

- --
Silicon Graphics Inc.

SGI acknowledges CERT Advisory CA-96.02 and is currently investigating.
No further information is available at this time.

As further information becomes available, additional advisories will
be available from ftp://sgigate.sgi.com.

- --
Solbourne (Grumman)

Solbourne have determined that Solbourne Computers are vulnerable.
A patch is not available and they recommend Solbourne customers install
BIND version 4.9.3.

- --
Sun Microsystems, Inc.

Sun Security Patches and Bulletins are available through your local
SunService and SunSoft Support Services organizations, via the
security-alert alias (security-alert@sun.com) and on SunSolve
Online:

        http://sunsolve1.sun.com/

SunOS 5.3/Solaris 2.3
- ---------------------
        101359-03   SunOS 5.3: DNS spoofing is possible per CERT CA-96.02
        101739-12   sendmail patch
        102167-03   nss_dns.so.1 rebuild for BIND 4.9.3
        103705-01   rpc.nisd_resolv rebuild for BIND 4.9.3

SunOS 5.4/Solaris 2.4
- ---------------------
        102479-02   SunOS 5.4: DNS spoofing is possible per CERT CA-96.02
        102066-11   sendmail patch
        102165-03   nss_dns.so.1 rebuild for BIND 4.9.3
        103706-01   rpc.nisd_resolv rebuild for BIND 4.9.3

SunOS 5.4_x86/Solaris 2.4_x86
- -----------------------------
        102480-02   SunOS 5.4_x86: DNS spoofing is possible per
                          CERT CA-96.02
        102064-10   sendmail patch
        102166-03   nss_dns.so.1 rebuild for BIND 4.9.3
        103707-01   rpc.nisd_resolv rebuild for BIND 4.9.3

SunOS 5.5/Solaris 2.5
- ---------------------
        103667-01   SunOS 5.5: DNS spoofing is possible per CERT CA-96.02
        102980-07   sendmail patch
        103279-02   nscd/nscd_nischeck rebuild for BIND 4.9.3
        103703-01   nss_dns.so.1 rebuild for BIND 4.9.3
        103708-01   rpc.nisd_resolv rebuild for BIND 4.9.3

SunOS 5.5_x86/Solaris 2.5_x86
- -----------------------------
        103668-01   SunOS 5.5_x86: DNS spoofing is possible per
                          CERT CA-96.02
        102981-07   sendmail patch
        103280-02   nscd/nscd_nischeck rebuild for BIND 4.9.3
        103704-01   nss_dns.so.1 rebuild for BIND 4.9.3
        103709-01   rpc.nisd_resolv rebuild for BIND 4.9.3

SunOS 5.5.1/Solaris 2.5.1
- -------------------------
        103663-01   SunOS 5.5.1: DNS spoofing is possible per CERT CA-96.02
        103594-03   sendmail patch
        103680-01   nscd/nscd_nischeck rebuild for BIND 4.9.3
        103683-01   nss_dns.so.1 rebuild for BIND 4.9.3
        103686-01   rpc.nisd_resolv rebuild for BIND 4.9.3

SunOS 5.5.1_ppc/Solaris 2.5.1_ppc
- ---------------------------------

103665-01	SunOS 5.5.1_ppc: DNS spoofing is possible per CERT CA-96.02
103596-03	sendmail patch
103682-01	nscd/nscd_nischeck rebuild for BIND 4.9.3
103685-01	nss_dns.so.1 rebuild for BIND 4.9.3
103688-01	rpc.nisd_resolv rebuild for BIND 4.9.3

SunOS 5.5.1_x86/Solaris 2.5.1_x86
- ---------------------------------

103664-01	SunOS 5.5.1_x86: DNS spoofing is possible per CERT CA-96.02
103595-03	sendmail patch
103681-01	nscd/nscd_nischeck rebuild for BIND 4.9.3
103684-01	nss_dns.so.1 rebuild for BIND 4.9.3
103687-01	rpc.nisd_resolv rebuild for BIND 4.9.3

- ---
The CERT Coordination Center wishes to thank Paul Vixie for his efforts in responding to this problem and his aid in developing this advisory.
- ---

If you believe that your system has been compromised, contact the CERT Coordination Center or your representative in the Forum of Incident Response and Security Teams (FIRST).

We strongly urge you to encrypt any sensitive information you send by email. The CERT Coordination Center can support a shared DES key and PGP. Contact the CERT staff for more information.

Location of CERT PGP key
ftp://info.cert.org/pub/CERT_PGP.key

CERT Contact Information
- ------------------------
Email cert@cert.org

Phone +1 412-268-7090 (24-hour hotline)
CERT personnel answer 8:30-5:00 p.m. EST (GMT-5)/EDT(GMT-4), and are on call for emergencies during other hours.

Fax +1 412-268-6989

Postal address
CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
USA

To be added to our mailing list for CERT advisories and bulletins, send your email address to
cert-advisory-request@cert.org

CERT publications, information about FIRST representatives, and other security-related information are available for anonymous FTP from
ftp://info.cert.org/pub/

CERT advisories and bulletins are also posted on the USENET newsgroup
comp.security.announce

==========
UPDATES

June 25, 1997
- -------------

If you are running BIND 8.1 you want to upgrade. The current version of BIND (8.8.1) is available by anonymous FTP from

ftp://ftp.isc.org/isc/bind/src/8.1.1

If you are still running BIND-4 rather than BIND-8, you need the

security patches contained in BIND 4.9.6. Available from

  ftp://ftp.isc.org/isc/bind/src/4.9.6/

The author of BIND encourages sites to switch to BIND-8.

~~~~~~
Revision History

Aug. 13, 1997 This advisory superseded by CA-97.22.
June 25, 1997 Appendix, Changed Vixie entry to point to Updates.
               Updates section - Current release information.
May 22, 1997 Updates section - noted current version of BIND and new location
                                for the BIND archives.
Aug. 30, 1996 Information previously in the README was inserted into the
               advisory.
Aug. 01, 1996 Appendix - updated Sun patch information
Apr. 08, 1996 Sec. I - added information about the next release of BIND
               and the IsValid program to the end of the section
Mar. 29, 1996 Appendix, Sun - added information
Feb. 27, 1996 Appendix, SGI - added an entry
Feb. 21, 1996 Appendix, IBM & Solbourne - added entries

-----BEGIN PGP SIGNATURE-----
Version: PGP for Personal Privacy 5.0
Charset: noconv

iQA/AwUBOBS+Hlr9kb5qlZHQEQLZkACg+G7DT+bLQvuP7tEV0k2htSHmgc0An2K9
Mryioy3iXYkXE05WHwxauFQL
=68Ml
-----END PGP SIGNATURE-----
~~~~~~