# CERT Advisory CA-2002-31 Multiple Vulnerabilities in BIND

Original release date: November 14, 2002
Last revised: Tue Apr 29 17:46:04 EST 2003
Source: CERT/CC

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

### Systems Affected

- Systems running various versions of BIND 4 and BIND 8

  Because the normal operation of most services on the Internet depends on the proper operation of DNS servers, other services could be affected if these vulnerabilities are exploited.

## Overview

Multiple vulnerabilities with varying impacts have been found in BIND, the popular domain name server and client library software package from the Internet Software Consortium (ISC).

Some of these vulnerabilities may allow remote attackers to execute arbitrary code with the privileges of the user running *named*, (typically root), or with the privileges of vulnerable client applications. The other vulnerabilities will allow remote attackers to disrupt the normal operation of DNS name service running on victim servers.

## I. Description

Multiple vulnerabilities have been found in BIND (Berkeley Internet Name Domain). One of these vulnerabilities (VU#852283) may allow remote attackers to execute arbitrary code with the privileges of the user running *named*, typically root. Other vulnerabilities (VU#229595, VU#581682) may allow remote attackers to disrupt the normal operation of your name server, possibly causing a crash. A vulnerability in the DNS resolver library (VU#844360) may allow remote attackers to execute arbitrary code with the privileges of applications that issue network name or address requests.

### BIND DNS Server Vulnerabilities

#### VU#852283 - Cached malformed SIG record buffer overflow

This vulnerability is a buffer overflow in *named*. It can occur when responses are constructed using previously-cached malformed SIG records. (SIG records are typically associated with cryptographically signed DNS data.) Exploitation of the vulnerability can lead to arbitrary code execution as the *named* uid, typically root.

The following versions of BIND are affected:

- BIND versions 4.9.5 to 4.9.10
- BIND versions 8.1, 8.2 to 8.2.6, and 8.3.0 to 8.3.3

#### VU#229595 - Overly large OPT record assertion

ISC BIND 8 fails to properly handle DNS lookups for non-existent sub-domains when overly large OPT resource records are appended to a query. When a non-existent domain (NXDOMAIN) response is constructed by a victim nameserver, an assertion may be triggered if the client passes a large UDP buffer size. This assertion will cause the running *named* to exit.

The following versions of BIND are affected:

- BIND versions 8.3.0 to 8.3.3

#### VU#581682 - ISC BIND 8 fails to properly de-reference cache SIG RR elements with invalid expiry times from the internal database

ISC's description of this vulnerability states:

*It is possible to de-reference a NULL pointer for certain signature expire values.*

The following versions of BIND are affected:

- BIND versions 8.2 to 8.2.6
- BIND versions 8.3.0 to 8.3.3.

### BIND DNS Resolver Vulnerabilities

### VU#844360 - Domain Name System (DNS) stub resolver libraries vulnerable to buffer overflows via network name or address lookups

The stub resolver library in BIND 4 contains buffer overflows in code that handles responses for network name and address requests. Note that these overflows are distinct from the issues discussed in CA-2002-19 and VU#738331.

The following DNS stub resolver libraries are known to be affected:

- BIND 4.9.2 through 4.9.10

The status of other resolver libraries derived from BIND 4 such as BSD libc, GNU glibc, and those used by System V UNIX systems is currently unknown. These issues map to CVE as follows:

> *VU#852283 - CAN-2002-1219*
> *VU#229595 - CAN-2002-1220*
> *VU#581682 - CAN-2002-1221*
> *VU#844360 - CAN-2002-0029*

## II. Impact

### VU#852283 - Cached malformed SIG record buffer overflow

A remote attacker could execute arbitrary code on the nameserver with the privileges of the *named* uid, typically root.

### VU#229595 - Overly large OPT record assertion

A remote attacker can disrupt the normal operation of your name server, possibly causing a crash.

### VU#581682 - ISC BIND 8 fails to properly de-reference cache SIG RR elements with invalid expiry times from the internal database

A remote attacker can disrupt the normal operation of your name server, possibly causing a crash.

### VU#844360 - Domain Name System (DNS) stub resolver libraries vulnerable to buffer overflows via network name or address lookups

A remote attacker could execute arbitrary code with the privileges of the application that made the request or cause a denial of service. The attacker would need to control DNS responses possibly by spoofing the responses or by gaining sufficient access to a DNS server.

## III. Solution

**Apply a patch from your vendor.**

Appendix A 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. Please contact your vendor directly.

If a vendor patch is not available, you may wish to consider applying the patches ISC has produced:

> *BIND 8.3.3 - http://www.isc.org/products/BIND/patches/bind833.diff*
>
> *BIND 8.2.6 - http://www.isc.org/products/BIND/patches/bind826.diff*
>
> *BIND 4.9.10 - http://www.isc.org/products/BIND/patches/bind4910.diff*

For VU#844360, the BIND 4 *libresolv* buffer overflows, an upgrade to a corrected version of the DNS resolver libraries will be required.

Note that DNS resolver libraries can be used by multiple applications on most systems. It may be necessary to upgrade or apply multiple patches and then recompile statically linked applications.

Applications that are *statically* linked must be recompiled using patched resolver libraries. Applications that are *dynamically* linked do not need to be recompiled; however, running services need to be restarted in order to use the patched resolver libraries.

System administrators should consider the following process when addressing this issue:

1. Patch or obtain updated resolver libraries.
2. Restart any dynamically linked services that use the resolver libraries.
3. Recompile any statically linked applications using the patched or updated resolver libraries.

### Workarounds

VU#852283 - Cached malformed SIG record buffer overflow

VU#229595 - Overly large OPT record assertion

VU#581682 - ISC BIND 8 fails to properly dereference cache SIG RR elements with invalid expiry times from the internal database

One potential workaround to limit exposure to the vulnerabilities in *named* is to disable recursion on any nameserver responding to DNS requests made by untrusted systems. As mentioned in Securing an Internet Name Server":

> *Disabling recursion puts your name servers into a passive mode, telling them never to send queries on behalf of other name servers or resolvers. A totally non-recursive name server is protected from cache poisoning, since it will only answer queries directed to it. It doesn't send queries, and hence doesn't cache any data. Disabling recursion can also prevent attackers from bouncing denial of services attacks off your name server by querying for external zones.*

Non-recursive nameservers should be much more resistant to exploitation of the server vulnerabilites listed above.

### Additional Countermeasures

ISC recommends upgrading to BIND version 9.2.1. BIND version 9.2.1 is available from: http://www.isc.org/products/BIND/bind9.html.

Note that the upgrade from previous versions of BIND may require additional site reconfiguration.

## 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.

### Alcatel
Following CERT advisory CA-2002-31 on security vulnerabilities in the ISC BIND implementation, Alcatel has conducted an immediate assessment to determine any impact this may have on our portfolio. A first analysis has shown that the following products (OmniSwitch 6600, 7700, 8800) may be impacted. Customers may wish to contact their support for more details. The security of our customers' networks is of highest priority for Alcatel. Therefore we continue to test our product portfolio against potential ISC BIND security vulnerabilities and will provide updates if necessary.

### Apple
Affected Systems:  Mac OS X and Mac OS X Server with BIND versions 8.1, 8.2 to 8.2.6, and 8.3.0 to 8.3.3

Mitigating Factors:  BIND is not enabled by default on Mac OS X or Mac OS X Server

This is addressed in Security Update 2002-11-21
http://www.apple.com/support/security/security_updates.html

### Conectiva
Conectiva Linux 6.0 is affected by this. Updated packages are available at our ftp server: ftp://atualizacoes.conectiva.com.br/6.0/RPMS/bind-8.2.6-1U60_2cl.i386.rpm
ftp://atualizacoes.conectiva.com.br/6.0/RPMS/bind-chroot-8.2.6-1U60_2cl.i386.rpm
ftp://atualizacoes.conectiva.com.br/6.0/RPMS/bind-devel-8.2.6-1U60_2cl.i386.rpm
ftp://atualizacoes.conectiva.com.br/6.0/RPMS/bind-devel-static-8.2.6-1U60_2cl.i386.rpm
ftp://atualizacoes.conectiva.com.br/6.0/RPMS/bind-doc-8.2.6-1U60_2cl.i386.rpm
ftp://atualizacoes.conectiva.com.br/6.0/RPMS/bind-utils-8.2.6-1U60_2cl.i386.rpm

An advisory about this vulnerability is pending and should be sent to our security mailing list and published in our web site during the day (Nov 14th).

### Cray Inc.
Cray Inc. may be vulnerable and has opened spr 723892 to investigate.

### Debian GNU/Linux
Debian (among other GNU/Linux distributors) was very unhappe to learn that ISC knew about this vulerability since mid October and that the advisory was released without patches, so only paying members of the ISC forum were able to provide updates to their customers. However, after the patches were finally released to the public, Debian was able to provide fixed packages as well. They are announced in DSA 196 .

### FreeBSD
Please see FreeBSD-SA-02:43.bind.

### GNU glibc
Version 2.3.1 of the GNU C Library is vulnerable. Earlier versions are also vulnerable. The following patch has been installed into the CVS sources, and should appear in the next version of the GNU C Library. This patch is also available from the following URL:

<http://sources.redhat.com/cgi-bin/cvsweb.cgi/libc/resolv/nss_dns/

dns-network.c.diff?r1=1.17&r2=1.15&cvsroot=glibc>

```
2002-11-18  Roland McGrath

        * resolv/nss_dns/dns-network.c (getanswer_r): In BYNAME case, search
        all aliases for one that matches the ".IN-ADDR.ARPA" form.
        Do the parsing inline instead of copying strings and calling
        inet_network, and properly skip all alias names not matching the form.

2002-11-14  Paul Eggert

        * resolv/nss_dns/dns-network.c (getanswer_r): Check for buffer
        overflow when skipping the question part and when unpacking aliases.

===================================================================
RCS file: /cvs/glibc/libc/resolv/nss_dns/dns-network.c,v
retrieving revision 1.15
retrieving revision 1.17
diff -u -r1.15 -r1.17
--- libc/resolv/nss_dns/dns-network.c        2002/10/17 21:49:12        1.15
+++ libc/resolv/nss_dns/dns-network.c        2002/11/19 06:40:16        1.17
@@ -283,7 +283,15 @@

   /* Skip the question part.  */
   while (question_count-- > 0)
-    cp += __dn_skipname (cp, end_of_message) + QFIXEDSZ;
+    {
+      int n = __dn_skipname (cp, end_of_message);
+      if (n < 0 || end_of_message - (cp + n) < QFIXEDSZ)
+       {
+         __set_h_errno (NO_RECOVERY);
+         return NSS_STATUS_UNAVAIL;
+       }
+      cp += n + QFIXEDSZ;
+    }

   alias_pointer = result->n_aliases = &net_data->aliases[0];
   *alias_pointer = NULL;
@@ -344,64 +352,94 @@
               return NSS_STATUS_UNAVAIL;
             }
           cp += n;
-          *alias_pointer++ = bp;
-          n = strlen (bp) + 1;
-          bp += n;
-          linebuflen -= n;
-          result->n_addrtype = class == C_IN ? AF_INET : AF_UNSPEC;
-          ++have_answer;
+         if (alias_pointer + 2 < &net_data->aliases[MAX_NR_ALIASES])
+           {
+             *alias_pointer++ = bp;
+             n = strlen (bp) + 1;
+             bp += n;
+             linebuflen -= n;
+             result->n_addrtype = class == C_IN ? AF_INET : AF_UNSPEC;
+             ++have_answer;
+           }
         }
     }

   if (have_answer)
     {
-      char *tmp;
-      int len;
-      char *in, *cp, *rp, *wp;
-      int cnt, first_flag;
-
       *alias_pointer = NULL;
       switch (net_i)
         {
         case BYADDR:
-          result->n_name = result->n_aliases[0];
+          result->n_name = *result->n_aliases++;
           result->n_net = 0L;
-          break;
-        case BYNAME:
-          len = strlen (result->n_aliases[0]);
-          tmp = (char *) alloca (len + 1);
-          tmp[len] = 0;
-          wp = &tmp[len - 1];
-
-          rp = in = result->n_aliases[0];
-          result->n_name = ans;
```

```
-
-          first_flag = 1;
-          for (cnt = 0; cnt < 4; ++cnt)
-            {
-              char *startp;
+          return NSS_STATUS_SUCCESS;

-              startp = rp;
-              while (*rp != '.')
-                ++rp;
-              if (rp - startp > 1 || *startp != '0' || !first_flag)
-                {
-                  first_flag = 0;
-                  if (cnt > 0)
-                    *wp-- = '.';
-                  cp = rp;
-                  while (cp > startp)
-                    *wp-- = *--cp;
-                }
-              in = rp + 1;
-            }
-
-          result->n_net = inet_network (wp);
+        case BYNAME:
+          {
+            char **ap = result->n_aliases++;
+            while (*ap != NULL)
+              {
+                /* Check each alias name for being of the forms:
+                   4.3.2.1.in-addr.arpa                = net 1.2.3.4
+                   3.2.1.in-addr.arpa                 = net 0.1.2.3
+                   2.1.in-addr.arpa                 = net 0.0.1.2
+                   1.in-addr.arpa                 = net 0.0.0.1
+                */
+                uint32_t val = 0;        /* Accumulator for n_net value.  */
+                unsigned int shift = 0; /* Which part we are parsing now.  */
+                const char *p = *ap; /* Consuming the string.  */
+                do
+                  {
+                    /* Match the leading 0 or 0[xX] base indicator.  */
+                    unsigned int base = 10;
+                    if (*p == '0' && p[1] != '.')
+                      {
+                        base = 8;
+                        ++p;
+                        if (*p == 'x' || *p == 'X')
+                          {
+                            base = 16;
+                            ++p;
+                            if (*p == '.')
+                              break; /* No digit here.  Give up on alias.  */
+                          }
+                        if (*p == '\0')
+                          break;
+                      }
+
+                    uint32_t part = 0; /* Accumulates this part's number.  */
+                    do
+                      {
+                        if (isdigit (*p) && (*p - '0' < base))
+                          part = (part * base) + (*p - '0');
+                        else if (base == 16 && isxdigit (*p))
+                          part = (part << 4) + 10 + (tolower (*p) - 'a');
+                        ++p;
+                      } while (*p != '\0' && *p != '.');
+
+                    if (*p != '.')
+                      break;        /* Bad form.  Give up on this name.  */
+
+                    /* Install this as the next more significant byte.  */
+                    val |= part << shift;
+                    shift += 8;
+                    ++p;
+
+                    /* If we are out of digits now, there are two cases:
+                       1. We are done with digits and now see "in-addr.arpa".
+                       2. This is not the droid we are looking for.  */
+                    if (!isdigit (*p) && !strcasecmp (p, "in-addr.arpa"))
+                      {
+                        result->n_net = val;
+                        return NSS_STATUS_SUCCESS;
+                      }
+
+                    /* Keep going when we have seen fewer than 4 parts.  */
```

```
+                 } while (shift < 32);
+             }
+         }
          break;
        }
-
-      ++result->n_aliases;
-      return NSS_STATUS_SUCCESS;
     }

   __set_h_errno (TRY_AGAIN);
```

### Hewlett-Packard Company
SOURCE: Hewlett-Packard Company Software Security Response team x-ref: SSRT2408

At the time of writing this document, Hewlett Packard is currently investigating the potential impact to HP's released Operating System software products. As further information becomes available HP will provide notice of the availability of any necessary patches through standard security bulletin announcements and be available from your normal HP Services support channel.

### IBM Corporation
The AIX operating system is vulnerable to the named and DNS resolver issues in releases 4.3.3, 5.1.0 and 5.2.0. The following APARs are available:

> *AIX 4.3.3 APAR IY37088 (available)*
> *AIX 5.1.0 APAR IY37091 (available)*
> *AIX 5.2.0 APAR IY37289 (available)*

### MandrakeSoft
Linux-Mandrake 7.2 and Single Network Firewall 7.2 are the only supported distributions to ship with BIND8; all other supported distributions ship with BIND9 and are thus not vulnerable. Updates for Linux-Mandrake 7.2 and Single Network Firewall 7.2 will be made available shortly. These updates will consist of BIND9 packages and patched BIND8 packages, although MandrakeSoft recommends that everyone able to, upgrade to the BIND9 packages.

### MetaSolv
MetaSolv Statement ref:CERTR Advisory CA-2002-31

The BIND code embedded in the DNS Server (Based on ISC BIND 8.2.3) on both MetaSolv Policy Services 4.1 and 4.2 (base) are partially vulnerable to CERTR Advisory CA-2002-31. This issue is being tracked by MetaSolv under Case #28231. In particular:

VU#844360 - Domain Name System (DNS) stub resolver libraries vulnerable to buffer overflows via network name or address lookups (VU#852283 - CAN-2002-1219 / VU#229595 - CAN-2002-1220 / VU#581682 - CAN-2002-1221/ VU#844360 - CAN-2002-0029) was addressed in Policy Services 4.2 Service Pack 1 efix 1. The vulnerability can be avoided by upgrading to Policy Services 4.2 Service Pack 1 efix 1 from MetaSolv Policy Services 4.1 and 4.2 (base). The efix includes all ISC sanctioned patches to BIND 8.2.6. to remedy this vulnerability. Please contact MetaSolv Global Customer Care (supporthd @metasolv.com) for assistance.

VU#229595 - Overly large OPT record assertion on BIND 8.3.x does not affect the current distribution as the base is on ISC BIND 8.2.6 and the ISC Sanctioned Patches to 8.2.6 in 4.2 Service Pack 1 efix 1. No action is required in Policy Services 4.1 and 4.2 (base) or Policy Services 4.2 Service Pack 1 efix 1 for this vulnerability.

VU#852283 - Cached malformed SIG record buffer overflow and VU#581682 - ISC BIND 8 fails to properly de-reference cache SIG RR elements with invalid expiry times from the internal database. The ISC sanctioned library changes to 8.2.6. have been applied to 4.2 Service Pack 1 and are currently undergoing load and integration testing and will be available as Policy Services 4.2 Service Pack 1 efix 2 on 11/22/02. Please contact MetaSolv Global Customer Care (supporthd@metasolv.com) for availability and assistance.

### Microsoft Corporation
Microsoft products do not use the program in question. Microsoft products are not affected by this issue.

### MontaVista Software
MontaVista ships BIND 9, thus is not vulnerable to these advisories.

### Nominum, Inc.
Nominum "Foundation" Authoritative Name Server (ANS) is not affected by this vulnerability. Also, Nominum "Foundation" Caching Name Server (CNS) is not affected by this vulnerability. Nominum's commercial DNS server products, which are part of Nominum "Foundation" IP Address Suite, are not based on BIND and do not contain any BIND code, and so are not affected by vulnerabilities discovered in any version of BIND.

### Nortel Networks
NetID version 4.3.1 and below is affected by the vulnerabilities identified in CERT/CC Advisory CA-2002-31. A bulletin and patched builds are available from the following Nortel Networks support contacts:

North America: 1-800-4NORTEL or 1-800-466-7835

Europe, Middle East and Africa: 00800 8008 9009, or +44 (0) 870 907 9009

Optivity NMS is not affected.

### Openwall Project
BIND 4.9.10-OW2 includes the patch provided by ISC and thus has the two vulnerabilities affecting BIND 4 fixed. Previous versions of BIND 4.9.x-OW patches, if used properly, significantly reduced the impact of the "named" vulnerability. The patches are available at their usual location:

http://www.openwall.com/bind/

A patch against BIND 4.9.11 will appear as soon as this version is officially released, although it will likely be effectively the same as the currently available 4.9.10-OW2. It hasn't been fully researched whether the resolver code in glibc, and in particular on Openwall GNU/*/Linux, shares any of the newly discovered BIND 4 resolver library vulnerabilities. Analysis is in progress.

### Red Hat Inc.
Older releases (6.2, 7.0) of Red Hat Linux shipped with versions of BIND which may be vulnerable to these issues however a Red Hat security advisory in July 2002 upgraded all our supported distributions to BIND 9.2.1 which is not vulnerable to these issues.

All users who have BIND installed should ensure that they are running these updated versions of BIND.

http://rhn.redhat.com/errata/RHSA-2002-133.html Red Hat Linux
http://rhn.redhat.com/errata/RHSA-2002-119.html Advanced Server 2.1

### Sun Microsystems
The Solaris DNS resolver library (libresolv(3LIB)) is affected by VU#844360 in the following supported versions of Solaris:

> *Solaris 2.6*

The Solaris BIND (in.named(1M)) daemon is affected by VU#852283 and VU#581682 in the following supported versions of Solaris:

> *Solaris 7, 8, and 9*

The Solaris BIND (in.named(1M)) daemon is affected by VU#229595 in the following supported versions of Solaris:

> *Solaris 9*

Patches are being generated for all of the above releases. Sun will be publishing a Sun Alert for this issue at the following location shortly:

> *http://sunsolve.Sun.COM/pub-cgi/retrieve.pl?doc=fsalert%2F48818*

The patches will be available from:

> *http://sunsolve.sun.com/securitypatch*

### Xerox
A response to this vulnerability [VU#229595, VU#844360, VU#852283] is available from our web site: http://www.xerox.com/security.

## Appendix B. - References


1. "Securing an Internet Name Server" - http://www.cert.org/archive/pdf/dns.pdf
2. "Internet Security Systems Security Advisory - Multiple Remote Vulnerabilities in BIND4 and BIND8" - http://bvlive01.iss.net/issEn/delivery/xforce/alertdetail.jsp?oid=21469
3. "BIND Vulnerabilities" - http://www.isc.org/products/BIND/bind-security.html
4. "RFC2671 - Extension Mechanisms for DNS (EDNS0)" - ftp://ftp.isi.edu/in-notes/rfc2671.txt


---

*Internet Security Systems* publicly reported the following issues VU#852283, VU#229595, and VU#581682.

We thank ISC for their cooperation.

---

Author: Ian A. Finlay, Jeffrey S. Havrilla, Art Manion, and Jeffrey J. Carpenter.

Revision History

November 14, 2002: Initial release
November 14, 2002: Added vendor statement for MandrakeSoft
November 14, 2002: Added vendor statement for Cray Inc.
November 14, 2002: Re-worded VU#844360 overview, description, and impact, added indentation
November 14, 2002: Added vendor statement for Microsoft Corporation
November 14, 2002: Added vendor statement for Debian GNU/Linux
November 15, 2002: Added vendor statement for IBM
November 15, 2002: Added vendor statement for MetaSolv
November 15, 2002: Added vendor statement for Sun
November 15, 2002: Added vendor statement for Nortel
November 21, 2002: Added vendor statement for Apple
December 03, 2002: Revised vendor statement for Nortel (note their update was sent on Nov 27, 2002)
December 09, 2002: Revised vendor statement for IBM
February 25, 2003: Added vendor statement for Alcatel
February 26, 2003: Added vendor statement for glibc
February 27, 2003: Updated vendor statement for IBM
April 29, 2003: Added vendor statement for Xerox