CERT Advisory CA-2000-20 Multiple Denial-of-Service Problems in ISC BIND

Original release date: November 13, 2000
Last updated: August 08, 2001
Source: CERT/CC

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

Systems Affected

- Systems running Internet Software Consortium (ISC) BIND version 8.2 through 8.2.2-P6
- Systems running name servers derived from BIND version 8.2 through 8.2.2-P6

Overview

The CERT Coordination Center has recently learned of two serious denial-of-service vulnerabilities in the Internet Software Consortium's (ISC) BIND software.

The first vulnerability is referred to by the ISC as the "zxfr bug" and affects ISC BIND version 8.2.2, patch levels 1 through 6. The second vulnerability, the "srv bug", affects ISC BIND versions 8.2 through 8.2.2-P6. Derivatives of the above code sets should also be presumed vulnerable unless proven otherwise.

I. Description

The Internet Software Consortium, the maintainer of BIND, the software used to provide domain name resolution services, has recently posted information about several denial-of-service vulnerabilities. If exploited, any of these vulnerabilities could allow remote intruders to cause site DNS services to be stopped.

For more information about these vulnerabilities and others, please see

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

Two vulnerabilities in particular have been categorized by both the ISC and the CERT/CC as being serious.

VU#715973 - ISC BIND 8.2.2-P6 vulnerable to DoS via compressed zone transfer, aka the "zxfr bug" (CVE-2000-0887)

Using this vulnerability, attackers on sites which are permitted to request zone transfers can force the *named* daemon running on vulnerable DNS servers to crash, disrupting name resolution service until the *named* daemon is restarted. The only preconditions for this attack to succeed is that a compressed zone transfer (ZXFR) request be made from a site allowed to make any zone transfer request (not just ZXFR), and that a subsequent name service query of an authoritative and non-cached record be made. The time between the attack and the crash of *named* may vary from system to system.

This vulnerability has been discussed in public forums. The ISC has confirmed that all platforms running version 8.2.2 of the BIND software prior to patch level 7 are vulnerable to this attack.

VU#198355 - ISC BIND 8.2.2-P6 vulnerable to DoS when processing SRV records, aka the "srv bug" (CVE-2000-0888)

This vulnerability can cause affected DNS servers running *named* to go into an infinite loop, thus preventing further name requests to be handled. This can happen if an SRV record (defined in
RFC2782) is sent to the vulnerable server.

Microsoft's Windows 2000 Active Directory service makes extensive use of SRV records and is reportedly capable of triggering this bug in the course of normal operations. This is not, however, a vulnerability in Microsoft Active Directory. ***Any network client capable of sending SRV records to vulnerable name server systems can exercise this vulnerability.***

The CERT/CC has not received any direct reports of either of these vulnerabilities being exploited to date.

Both vulnerabilities can be used by malicious users to break the DNS services being offered at all exposed sites on the Internet. System administrators are strongly recommended to upgrade their DNS software with either ISC's current distribution or their vendor-supplied software. See the Solution and Vendor Information sections of this document for more details.

II. Impact

Domain name resolution services (DNS) can be disabled on affected servers from arbitrary remote hosts.

III. Solution

Apply a patch from your vendor

The CERT/CC recommends that all users of ISC BIND upgrade to the recently-released BIND 8.2.2-P7, which patches both of the vulnerabilities discussed in this document. Sites running vendor-specific distributions of domain name resolution software should check the Vendor Information section below for more specific information on how to upgrade to non-vulnerable software.

Restrict zone transfers to trusted hosts

If it is not possible to immediately upgrade systems affected by the "zxfr bug", the ISC suggests not allowing zone transfers from untrusted hosts. This action, however, will not mitigate against the effects of an attack using the "srv bug".

Although it has been reported that not allowing recursive queries may help mitigate against the "zxfr" vulnerability, ISC has indicated that this is not the case.

Appendix A. Vendor Information

The Internet Software Consortium

For the latest information regarding these vulnerabilities, please consult the ISC web site at:

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

Caldera

Our advisory is available at:

http://www.calderasystems.com/support/security/advisories/CSSA-2000-040.0.txt
Updated packages are available from

OpenLinux Desktop 2.3
ftp://ftp.calderasystems.com/pub/updates/OpenLinux/2.3/current
9d8429f25c5fb3bebe2d66b1f9321e61 RPMS/bind-8.2.2p7-1.i386.rpm
0e958eb01f40826f000d779dbe6b8cb3 RPMS/bind-doc-8.2.2p7-1.i386.rpm
866ff74c77e9c04a6abcddcc11dbe17b RPMS/bind-utils-8.2.2p7-1.i386.rpm
6a545924805effbef01de74e34ba005e SRPMS/bind-8.2.2p7-1.src.rpm

OpenLinux eServer 2.3
ftp://ftp.calderasystems.com/pub/updates/eServer/2.3/current
379c4328604b4491a8f3d0de44e42347 RPMS/bind-8.2.2p7-1.i386.rpm
b428b824c8b67f2d8d4bf53738a3e7e0 RPMS/bind-doc-8.2.2p7-1.i386.rpm
28311d630281976a870d38abe91f07fb RPMS/bind-utils-8.2.2p7-1.i386.rpm
6a545924805effbef01de74e34ba005e SRPMS/bind-8.2.2p7-1.src.rpm

OpenLinux eDesktop 2.4
ftp://ftp.calderasystems.com/pub/updates/eDesktop/2.4/current
c37b6673cc9539e592013ac114846940 RPMS/bind-8.2.2p7-1.i386.rpm
bbe0d7e317fde0d47cba1384f6d4b635 RPMS/bind-doc-8.2.2p7-1.i386.rpm
5c28dd5641a4550c03e9859d945a806e RPMS/bind-utils-8.2.2p7-1.i386.rpm
6a545924805effbef01de74e34ba005e SRPMS/bind-8.2.2p7-1.src.rpm

Compaq Computer Corporation

SOURCE: Compaq Services Software Security Response Team

```
......................................................................
 COMPAQ COMPUTER CORPORATION

......................................................................
  CERT-2000-20 - BIND 8 The "zxfr bug"
                              X-REF: SSRT1-38U, CERT-2000-20
......................................................................
       Compaq Tru64 UNIX V5.1           -
                                   patch:  SSRT1-66U_v5.1.tar.Z

       Compaq Tru64 UNIX V5.0 & V5.0a   -
                            V5.0   patch: SSRT1-68U_v5.0.tar.Z
                            V5.0a  patch: SSRT1-68U_v5.0a.tar.Z

       Compaq Tru64 UNIX V4.0D/F/G              - Not Vulnerable
       TCP/IP Services for Compaq OpenVMS       - Not Vulnerable

......................................................................
CERT02000-20 - BIND 8 The "srv bug"
                             X-REF: SSRT1-38U, CERT CA2000-20
......................................................................
       Compaq Tru64 UNIX V5.1           -
                                   patch: SSRT1-66U_v5.1.tar.Z

       Compaq Tru64 UNIX V5.0 & V5.0a   -
                            V5.0   patch: SSRT1-68U_v5.0.tar.Z
                            V5.0a  patch: SSRT1-68U_v5.0a.tar.Z

       Compaq Tru64 UNIX V4.0D/F/G              - Not Vulnerable
       TCP/IP Services for Compaq OpenVMS        - Not Vulnerable

 Compaq will provide notice of the completion/availability of the
 patches through AES services (DIA, DSNlink FLASH), the Security
 mailing list, and be available from your normal Compaq Support
 channel. You may subscribe to the Security mailing list at:

http://www.support.compaq.com/patches/mailing-list.shtml
```

Conectiva

Please see Conectiva Linux Security Announcement CLSA-2000:339 at:

http://listserv.securityportal.com/SCRIPTS/WA-SECURITYPORTAL.EXE?A1=ind0011&L=linux-security#27

Note: Conectiva Linux Security Announcement CLSA-2000:338, also regarding this issue, had a packaging error in it. Users who downloaded updates based on CLSA-2000:338 should see CLSA-2000:339 for further information.

Debian

Please see Debian Security notice 20001112, bind at:

http://www.debian.org/security/2000/20001112

FreeBSD

All versions of FreeBSD after 4.0-RELEASE (namely 4.1-RELEASE, 4.1.1-RELEASE and the forthcoming 4.2-RELEASE) are not vulnerable to this bug since they include versions of BIND 8.2.3. FreeBSD 4.0-RELEASE and earlier are vulnerable to the reported problems since they include an older version of BIND, and an update to a non-vulnerable version is scheduled to be committed to FreeBSD 3.5.1-STABLE in the next few days.

[CERT/CC Addendum: FreeBSD has published an advisory regarding this issue at
ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-01:10.bind.asc]

Fujitsu

Fujitsu's UXP/V is not vulnerable to these bugs because we support a different version of BIND.

Hewlett-Packard

HP is vulnerable to the SRV issue and patches are available, see HP Security Bulletin #144.

[CERT/CC Addendum: To locate this HP Security Bulletin online, please visit
http://itrc.hp.com and search for "HPSBUX0102-144". Please note that registration may be required to access this document.]

IBM

IBM has reported to the CERT/CC that AIX is vulnerable to the bugs described in this document. IBM initially released an e-patch in APAR IY14512.

IBM has posted an e-fix for the BIND denial-of-service vulnerabilities to
ftp.software.ibm.com/aix/efixes/security. See the README file in this ftp directory for additional information.

Also, IBM has posted an e-fix to this same site that contains libc.a library that incorporates a fix to the BIND vulnerabilities and the recent locale subsystem format string vulnerability discovered by Ivan Arce of CORE, and discussed on Bugtraq. The e-fix for BIND must be downloaded and installed before implementing this e-fix. See the same README file for details.

Immunix

Immunix Linux versions 6.2 and 7.0 beta are both vulnerable, and a fix has been issued. See http://www.immunix.org/ImmunixOS/7.0-beta /updates/IMNX-2000-70-005-01 for the advisory and updated package information.

MandrakeSoft

Please see "MDKSA-2000:067: bind" at:

> http://www.linux-mandrake.com/en/security/MDKSA-2000-067.php3

Microsoft Corporation

We have had a chance to investigate these issues and we are not-vulnerable. This includes both Windows 2000 and Windows NT 4.0.

NetBSD

NetBSD is believed to be vulnerable to these problems; in response, NetBSD-current has been upgraded to 8.2.2-P7 and 8.2.2-P7 will be present in the forthcoming NetBSD 1.5 release.

RedHat

Please see "RHSA-2000:107-01: Updated bind packages fixing DoS attack", available at:

> http://www.redhat.com/support/errata/RHSA-2000-107.html

Slackware

Updated Slackware distributions for bind may be found at:

> ftp://ftp.slackware.com/pub/slackware/slackware-current/slakware/n1/bind.tgz

SuSE Inc

SuSE Linux has published a Security Announcement regarding these vulnerabilities. For further information, please visit:

> http://www.suse.com/de/support/security/2000_045_bind8_txt.txt

---

The CERT Coordination Center thanks Mark Andrews, David Conrad, and Paul Vixie of the
ISC for developing a solution and assisting in the preparation of this advisory. We would also recognize the contribution of Olaf Kirch in helping us understand the exact nature of the "zxfr bug" vulnerability.

Author: This document was written by Jeffrey S. Havrilla and Jeffrey P. Lanza. Feedback on this advisory is appreciated.

Revision History

```
Nov 13, 2000: Initial release
Nov 13, 2000: Added information regarding Immunix
Nov 13, 2000: Corrected typographical error in title
Nov 14, 2000: Updated RedHat and Microsoft sections
Nov 16, 2000: Added vendor info for IBM AIX and SuSE Linux
Nov 16, 2000: Added references for each vulnerability
Nov 22, 2000: Ammended statement from HP
Nov 28, 2000: Ammended statement from IBM
Feb 28, 2001: Updated Compaq statement; Tru64 Unix is affected
May 10, 2001: Updated HP statement
Jul 18, 2001: Added statement for Fujitsu (statement received on 12/22/00)
Aug 08, 2001: Fixed CVE references, added references to VU#715973 and VU#198355
```