CERT Advisory CA-1996-04 Corrupt Information from Network Servers

Original issue date: February 22, 1996
Last revised: April 28, 1998
Corrected URL for obtaining RFCs. Removed obsolete references to a latest_sw_versions directory.

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

The CERT Coordination Center has received reports of intruders exploiting systems by corrupting data provided by a Domain Name Service (DNS) server. Although these reports have focused only on DNS, this vulnerability could apply to any network service from which data is received and subsequently used.

Section III.A contains a pointer to two subroutines that address the DNS problem. These subroutines, written in the C programming language, can be used to validate host names and IP addresses according to RFCs 952 and 1123, as well as names containing characters drawn from common practice, namely "_" and "/".

In the specific case of sendmail, the problem has already been addressed by patches (see Section III.B).

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

ftp://ftp.isi.edu/in-notes/rfc952.txt

ftp://ftp.isi.edu/in-notes/rfc1123.txt

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

The latest release of Bind is available from:

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

I. Description

Information provided by an information server may be of a form that could cause programs to operate in unexpected ways. The subroutines and programs transferring data from that information server could check the data for correctness of form; however, programs that *use* that data are ultimately responsible for ensuring adherence to the documents that define the correct form.

For example, consider a program that uses the host name returned by gethostbyname() as part of the string given to the popen() or system() subroutines. Because gethostbyname() may use an information server beyond your control, the data returned could be of a form that causes the popen() or system() subroutines to execute other commands besides the command specified by that program.

This advisory speaks to a specific instance of a problem caused by the information returned by DNS, but information from any server should be checked for validity. Examples of other information servers are YP, NIS, NIS+, and netinfo.

II. Impact

Programs that do not check data provided by information servers may operate in unpredictable ways and give unexpected results. In particular, exploitation of this vulnerability may allow remote access by unauthorized users. Exploitation can also lead to root access by both local and remote users.

III. Solution

For programs that you write or have written, consider integrating the general solution in Section A below.

In the specific case of the sendmail mail delivery program, Eric Allman, the original author of sendmail, has produced patches that address the problem. Section B provides details about these, along with vendor information and additional steps you should take to protect sendmail.

A. General solution for Internet host names

Use the host name and IP address validation subroutines available at the locations listed below. Include them in all programs that use the result of the host name lookups in any way.

ftp://ftp.cert.org/pub/tools/ValidateHostname/IsValid.c

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

The IsValid.c file contains code for the IsValidHostname and IsValidIPAddress subroutines. This code can be used to check host names and IP addresses for validity according to RFCs 952 and 1123, well as names containing characters drawn from common practice, namely "_" and "/".

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

B. Specific solutions in the case of sendmail

Install a patch from your vendor when it becomes available (see B.1) or install Eric Allman's patch (B.2). In both cases, install the sendmail restricted shell program (B.3).

1. Install a patch from your vendor.

Below is a summary of the vendors who have reported status to us as of the date of this advisory. More complete information is provided in the appendix, which we will update as we receive more information.

If your vendor's name is not on this list, please contact the vendor directly.

Vendor or Source

Eric Allman
Hewlett-Packard Co.
IBM Corporation
Silicon Graphics Inc.
Sun Microsystems, Inc.

2. Install a patch to sendmail.

If you are presently running sendmail 8.6.12, there is a patch that makes version 8.6.13.

Similarly, if you are presently running sendmail 8.7.3, there is a patch that makes version 8.7.4.

The patches are available for anonymous FTP from

ftp://ftp.cert.org/pub/tools/sendmail/

ftp://ftp.cs.berkeley.edu/ucb/src/sendmail/

ftp://ftp.auscert.org.au/pub/mirrors/ftp.cs.berkeley.edu/ucb/sendmail/

ftp://ftp.cert.dfn.de/pub/tools/net/sendmail/

Checksums for the 8.6.13 release:

MD5 (sendmail.8.6.13.base.tar.Z) = e8cf3ea19876d9b9def5c0bcb793d241
MD5 (sendmail.8.6.13.cf.tar.Z) = 4492026fa9e750cd33974322cb5a6fb9
MD5 (sendmail.8.6.13.misc.tar.Z) = 7ec5d31656e93e08a3892f0ae542b674
MD5 (sendmail.8.6.13.xdoc.tar.Z) = e4d3caebcdc4912ed2ecce1a77e45712

Checksum for the 8.6.13 patch:

MD5 (sendmail.8.6.13.patch) = 6390b792cb5513ff622da8791d6d2073

Checksum for the 8.7.4 release:

MD5 (sendmail.8.7.4.tar.Z) = 4bf774a12752497527aae11e2bdbab36

Checksum for the 8.7.4 patch:

MD5 (sendmail.8.7.4.patch) = ef828ad91fe56e4eb6b0cacced864cd5

3. Run smrsh as additional protection for sendmail.

With all versions of sendmail, we recommend that you install and use the sendmail restricted shell program (smrsh). We urge you to do this whether you use the vendor's supplied sendmail, install sendmail yourself, or patch an earlier version of sendmail.

Beginning with version 8.7.1, smrsh is included in the sendmail distribution, in the subdirectory smrsh. See the RELEASE_NOTES file for a description of how to integrate smrsh into your sendmail configuration file.

Appendix A: Vendor Information

Below is information we have received from vendors concerning the vulnerability described in this advisory. If you do not see your vendor's name, please contact the vendor directly for information.

Eric Allman (original author of sendmail)

Install a patch to sendmail.

If you are presently running sendmail 8.6.12, there is a patch that makes version 8.6.13.

Similarly, if you are presently running sendmail 8.7.3, there is a patch that makes version 8.7.4.

The patches are available for anonymous FTP from

> ftp://ftp.cert.org/pub/tools/sendmail/
>
> ftp://ftp.cs.berkeley.edu/ucb/src/sendmail/
>
> ftp://ftp.auscert.org.au/pub/mirrors/ftp.cs.berkeley.edu/ucb/sendmail/
>
> ftp://ftp.cert.dfn.de/pub/tools/net/sendmail/

Checksums for the 8.6.13 release:

```
MD5 (sendmail.8.6.13.base.tar.Z) = e8cf3ea19876d9b9def5c0bcb793d241
MD5 (sendmail.8.6.13.cf.tar.Z) = 4492026fa9e750cd33974322cb5a6fb9
MD5 (sendmail.8.6.13.misc.tar.Z) = 7ec5d31656e93e08a3892f0ae542b67
MD5(sendmail.8.6.13.xdoc.tar.Z) = e4d3caebcdc4912ed2ecce1a77e45712
```

Checksum for the 8.6.13 patch:

```
MD5 (sendmail.8.6.13.patch) = 6390b792cb5513ff622da8791d6d2073
```

Checksum for the 8.7.4 release:

```
MD5 (sendmail.8.7.4.tar.Z) = 4bf774a12752497527aae11e2bdbab36
```

Checksum for the 8.7.4 patch:

```
MD5 (sendmail.8.7.4.patch) = ef828ad91fe56e4eb6b0cacced864cd5
```

Hewlett-Packard Company

Vulnerable, watch file for updates.

IBM Corporation

IBM is working on fixes for sendmail.

Silicon Graphics Inc.

It is **HIGHLY RECOMMENDED** that these measures be done on ALL SGI systems running IRIX 3.x, 4.x, 5.x and 6.x. The issue will be permanently corrected in a future release of IRIX.

**** IRIX 3.x ****

Silicon Graphics Inc, no longer supports the IRIX 3.x operating system and therefore has no patches or binaries to provide.

However, two possible actions still remain:
1) upgrade the system to a supported version of IRIX (see below) and then install the patch or
2) obtain the sendmail source code from anonymous FTP at ftp.cs.berkeley.edu and compile the program manually. Please, note that SGI will not assist with or support 3rd party sendmail programs.

**** IRIX 4.x ****

As of the date of this document, SGI does not have a IRIX 4.x binary replacement that addresses this particular issue. If in the future, a replacement binary is generated, additional advisory information will be provided.

However, two other possible actions are:
1) upgrade the system to a supported version of IRIX (see below) and then install the patch or
2) obtain the sendmail source code from anonymous FTP at ftp.cs.berkeley.edu and compile the program manually. Please, note that SGI will not assist with or support 3rd party sendmail programs.

**** IRIX 5.0.x, 5.1.x ****

For the IRIX operating systems versions 5.0.x and 5.1.x, an upgrade to 5.2 or better is required first. When the upgrade is completed, then the patches described in the following sections can be applied depending on the final version of the upgrade.

**** IRIX 5.2, 5.3, 6.0, 6.0.1, 6.1 ****

For the IRIX operating system versions 5.2, 5.3, 6.0, 6.0.1, and 6.1 an inst-able patch has been generated and made available via anonymous FTP and your service/support provider. The patch is number 1146 and will install on IRIX 5.2, 5.3, 6.0 and 6.0.1.

The SGI anonymous FTP site is sgigate.sgi.com (204.94.209.1) or its mirror, ftp.sgi.com. Patch 1146 can be found in the following directories on the FTP server:

~ftp/Security

or

~ftp/Patches/5.2
~ftp/Patches/5.3
~ftp/Patches/6.0
~ftp/Patches/6.0.1
~ftp/Patches/6.1

Checksums

The actual patch will be a tar file containing the following files:

Filename:	patchSG0001146
Algorithm #1 (sum -r):	15709 3 patchSG0001146
Algorithm #2 (sum):	16842 3 patchSG0001146
MD5 checksum:	055B660E1D5C1E38BC3128ADE7FC9A95

Filename:	patchSG0001146.eoe1_man
Algorithm #1 (sum -r):	26276 76 patchSG0001146.eoe1_man
Algorithm #2 (sum):	1567 76 patchSG0001146.eoe1_man
MD5 checksum:	883BC696F0A57B47F1CBAFA74BF53E81

Filename:	patchSG0001146.eoe1_sw
Algorithm #1 (sum -r):	61872 382 patchSG0001146.eoe1_sw
Algorithm #2 (sum):	42032 382 patchSG0001146.eoe1_sw
MD5 checksum:	412AB1A279A030192EA2A082CBA0D6E7

Filename:	patchSG0001146.idb
Algorithm #1 (sum -r):	39588 4 patchSG0001146.idb
Algorithm #2 (sum):	10621 4 patchSG0001146.idb
MD5 checksum:	259DD47E4574DAF9041675D64C39102E

Past SGI Advisories and security patches can be obtained via anonymous FTP from

ftp://sgigate.sgi.com

or its mirror

ftp://ftp.sgi.com

Sun Microsystems, Inc.

Included below is information concerning sendmail patches as outlined in Sun Microsystems Security Bulletin: #00133, 8 March 1996. The complete bulletin is available from ftp://ftp.cert.org/pub/vendors/sun/sun_bulletin_00133.

Here are our estimates for the availability of fixes incorporating into sendmail more strenuous checks against name-server-based attacks.

Note that the upcoming SunOS 4.1.x patches will represent the first backport of sendmail 8.6.x to those platforms, and will probably be assigned new patch numbers (instead of being recorded as revisions of the existing patches).

OS version	Est. date
5.6	in 5.6 FCS release
5.5.1	in 5.5.1 FCS release
5.5	Apr '96
5.4	Apr '96
5.3	Apr '96
4.1.4	May '96
4.1.3_U1	May '96
4.1.3	May '96

List of Current Sendmail Patches

Until the patches listed above are available, Sun recommends that every customer run the following sendmail patches on their systems.

A. Current sendmail patches

The latest sendmail patch for each supported version of SunOS is shown below. All current SunOS 5.x patches are based on sendmail V8; all SunOS 4.1.x patches are currently based on sendmail V5.

[Note that no sendmail patches exists for SunOS 5.5 and SunOS 5.5_x86. All earlier fixes were built into these releases.]

OS version	Patch ID	Released
5.4_x86	102064-05	19 Jan 96
5.4	102066-06	19 Jan 96
5.3	101739-08	19 Jan 96
4.1.4	102423-04	5 Oct 95
4.1.3_U1	101665-07	5 Oct 95
4.1.3	100377-22	5 Oct 95

Patch 100377-22 was issued jointly for SunOS 4.1.3 and SunOS 4.1.3c.

B. Obsolete sendmail patches

The following sendmail patches are now obsolete, and will no longer be maintained. Each is superseded by a patch listed above.

OS version	Patch ID	Released
5.4_x86	102320-01	26 May 95
5.4	102319-01	26 May 95
5.3	101235-01	1 May 95
5.3 (sic)	101371-04	9 Feb 94
4.1.4	102356-01	22 Feb 95
4.1.3_U1	101436-08	28 Oct 94
4.1.3	100224-13	28 Oct 94

Checksum Table

In the checksum table we show the BSD and SVR4 checksums and MD5 digital signatures for the compressed tar archives.

```
File            BSD          SVR4         MD5
Name            Checksum     Checksum     Digital Signature
--------------- -----------  ----------   --------------------------------
102064-05.tar.Z 08423   335  16923  669   2816EF17F40E2FA5E8260CD98D349875
102066-06.tar.Z 62613   385  52067  770   666E6D6075E40D2BFDB539830EF1BCDA
101739-08.tar.Z 60842   385  28595  770   369D4E0758672ADCDAD2219179B8A062
102423-04.tar.Z 40900   216  33691  432   022B546A882B42FF826FE28429B2EDD8
101665-07.tar.Z 44656   216  37045  431   86F942F8CCBAD905AB2AE8CA33490D2B
100377-22.tar.Z 39051   214  58206  427   7B55564E6104FABAD7283DAE1CDD3D4A
```

The checksums shown above are from the BSD-based checksum (on 4.1.x, /bin/sum; on SunOS 5.x, /usr/ucb/sum) and from the SVR4 version on on SunOS 5.x (/usr/bin/sum).

The CERT Coordination Center thanks Eric Allman of Pangaea Reference Systems, Andrew Gross of San Diego Supercomputer Center, Eric Halil of AUSCERT, Wolfgang Ley of DFN-CERT, and Paul Vixie for their support in the development of this advisory.

Revision History

```
Apr. 28, 1998 Corrected URL for obtaining RFCs. Removed obsolete references
              to a latest_sw_versions directory.
Sep. 24, 1997 Updated copyright statement
June 4, 1997  Updated the URL pointing to the current version of BIND.
Aug. 30, 1996 Incorporated changes from CA-96.04.README into the advisory.
July 01, 1996 Introduction - added pointer to BIND 4.9.4.
Mar. 29, 1996 Introduction - updated information about the next release
              of BIND
              Updates section - added isValid.c program information.
              Appendix, Sun - added information from Sun.
Feb. 28, 1996 Appendix, SGI - added information.
```