CERT Advisory CA-1997-04 talkd Vulnerability

Original issue date: January 27, 1997
Last revised: September 26, 1997
Updated copyright statement

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

The CERT Coordination Center has received reports of a vulnerability in *talkd(8)* program used by *talk(1)*. By constructing DNS data with particular characteristics, an intruder can remotely execute arbitrary commands with root privileges.

An exploitation script for this problem has been made publicly available, and we have received reports of successful root compromises involving the use of this script.

You may be aware of advisories that have been published by other response teams about this problem. Note that this advisory contains additional material and covers additional aspects of the vulnerability related to a broader set of problems of which this particular problem is only a specific instance.

The CERT/CC team recommends taking steps to solve the general problem (Sec. III.A) and installing a vendor patch to address this particular instance of the problem (Sec. III.B). Until you can install a patch, we urge you to disable the talkd program(s) at your site.

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

I. Description

The CERT Coordination Center has received information of a vulnerability in the *talkd(8)* program used by *talk(1)*. talk is a communication program that copies text from one user's terminal to that of another, possibly remote, user. talkd is the daemon that notifies a user that someone else wishes to initiate a talk conversation.

As part of the talk connection, talkd does a DNS lookup for the name of the host that the connection is being initiated from. Because there is insufficient bounds checking on the buffer where the hostname is stored, it is possible to overwrite the internal stack space of talkd.

It is possible to force talkd to execute arbitrary commands by carefully manipulating the hostname information. As talkd runs with root privileges, this may allow intruders to remotely execute arbitrary commands with these privileges.

This attack requires an intruder to be able to make a network connection to a vulnerable talkd program and provide corrupt DNS information to that host.

This type of attack is a particular instance of the problem described in CERT advisory CA-96.04, "Corrupt Information from Network Servers," available from

http://www.cert.org/advisories/CA-96.04.corrupt_info_from_servers

Sites that use BIND 4.9.4 Patch Level 1 or later are NOT vulnerable to the general class of hostname/ip-address-based buffer overflow attacks (including this specific problem).

Be aware that there are different versions of the talkd program. Depending on your system, the program may have any of the following names: talkd, otalkd, ntalkd.

To determine whether your site allows talk sessions, check /etc/inetd.conf:

```
# grep -i "^[a-z]*talk" /etc/inetd.conf
```

Note: An exploitation script for this problem has been made publicly available. The CERT/CC has received reports of successful root compromises involving the use of this script.

II. Impact

Intruders may be able to remotely execute arbitrary commands with root privileges. They do not need access to an account on the system to exploit this vulnerability.

III. Solution

There are several options available to avoid this problem. We recommend that all sites defend against the general class of problem (Sec. A) and also install a patch from your vendor (Sec. B). Until you can install a patch, we urge you to disable the talkd program(s) at your site (Sec C).

Note that disabling the talkd program will defend against the particular attack described in this advisory, but will not defend against the general class of network-based attacks that manipulate hostname/ip-address information to exploit a vulnerability.

A. Defend against the general class of problem

In the general case, the problem described in this advisory is one in which the attacker uses particular hostname/ip-address data to exploit a vulnerability. The exploitation script mentioned above uses the specific case of DNS attacks, but attackers can use other hostname/ip-address resolution methods, such as NIS, /etc/hosts, and so on.

If the following measures are in place for all hostname/address transformation techniques on your system, then your system would be immune not only to this particular talkd exploit, but also to the general class of hostname/ip-address-based buffer overflow attacks.

1. DNS-Based Attacks

To defend against a DNS-based attack, we encourage you to upgrade to BIND 4.9.4 Patch level 1 or later (or your vendor's equivalent). The reason is that BIND 4.9.4 Patch Level 1 conforms to the RFC (RFC 952) defining valid hostname syntax (described in CERT advisory CA-96.04, "Corrupt Information from Network Servers").

Keep in mind that an upgrade to 4.9.5 may require a sendmail upgrade because of the POSIX extensions in the latest version of BIND (described in CA-96.04). For the latest available version of sendmail, please consult the file

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

2. Other Network Information Services

For systems that rely on additional name/address transformation techniques (such as NIS, netinfo, and flat files like /etc/hosts), using the recommended version of BIND may be insufficient since DNS lookups--and therefore hostname/ip-address validation--may be bypassed in favor of the alternative technique (NIS, netinfo, etc). Thus, we also encourage sites and vendors to include in the suite of resolution techniques the same code that BIND uses to validate hostnames and IP addresses. This code is described in the next section.

3. In-house Software

Use the hostname and IP address validation subroutines available at the locations listed below. Include them in all programs that use the result of the hostname 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, as well as names containing characters drawn from common practice, namely "_" and "/".

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

IsValid.1	The Lex/Flex file containing the code for IsValidHostname and IsValidIPAddress MD5 (IsValid.1 = 2d35040aacae4fb12906eblb48957776
IsValid-raw.c	The C File created by running flex on is IsValid.l MD5 (IsValid-raw.c) = 367c77d3ef84bc63a5c23d90eeb69330
IsValid.c	The edited file created by internalizing variable and function definititions 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. Install a patch from your vendor

Below is a list of the vendors who have provided information. Details are in Appendix A of this advisory; we will update the appendix as we receive additional information.

If your vendor's name is not on this list, we have not received any information. Please contact the vendor directly.

Berkeley Software Design, Inc. (BSDI)
Cisco Systems
Data General Corporation
FreeBSD, Inc.
Hewlett-Packard Company
IBM Corporation
Linux
NEC Corporation
The Santa Cruz Operation, Inc. (SCO)
Silicon Graphics Inc. (SGI)
Solbourne (Grumman System Support)
Sun Microsystems, Inc.

C. Disable the talkd program(s)

Until you can install a vendor patch, disable any talkd programs found in /etc/inetd.conf by commenting out those lines and restarting inetd.

Example commands executed as root:

grep -i talk /etc/inetd.conf

talkdgramudpwaitroot/usr/etc/in.talkdin.talkd

Comment out *all* references to talkd, otalkd or ntalkd.
(Comments in # /etc/inetd.conf begin with "#".)

After editing /etc/inetd.conf, restart inetd. On many Unix systems, this is done by sending the inetd process a HUP signal.

For SYSV:

ps -ef | grep inetd | grep -v grep
kill -HUP {inetd PID}

For BSD:

ps -aux | grep inetd | grep -v grep
kill -HUP {inetd PID}

Note that disabling talkd will solve the specific problem discussed in this advisory. However it will not solve the general problem of network-based attacks that manipulate hostname/ip-address information to exploit a vulnerability.

Appendix A - Vendor Information

Below is a list of the vendors who have provided information for this advisory. We will update this appendix as we receive additional information. If you do not see your vendor's name, please contact the vendor directly.

Berkeley Software Design, Inc. (BSDI)

We have released an official patch (U210-035). It's available from our
patches@BSDI.COM mail-back server or via anonymous ftp at:

ftp://ftp.bsdi.com/bsdi/patches/patches-2.1/U210-035

Cisco Systems

Cisco MultiNet for OpenVMS - not vulnerable.

Data General Corporation

Data General is not vulnerable.

FreeBSD, Inc.

We have released an advisory dated 1997-01-18, FreeBSD-SA-96:21.
The advisory can be found at

ftp://freebsd.org/pub/CERT/advisories/FreeBSD-SA-96:21.talkd.asc

Patches are available at

ftp://freebsd.org/pub/CERT/patches/SA-96:21

Hewlett-Packard Company

HPSBUX9704-061
HEWLETT-PACKARD SECURITY BULLETIN: #00061
Description: Security Vulnerability in talkd
Security Bulletins are available from the HP Electronic
Support Center via electronic mail.
User your browser to get to the HP Electronic Support
Center page at:

http://us-support.external.hp.com (for US, Canada, Asia-Pacific, & Latin-America)
http://europe-support.external.hp.com (for Europe)

IBM Corporation

The version of talkd shipped with AIX is vulnerable to the conditions described in this advisory. The APARs listed below will be available shortly. It is recommended that the talkd daemon be turned off until the APARs are applied.

AIX 3.2:APAR IX65474
AIX 4.1:APAR IX65472
AIX 4.2:APAR IX65473

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://service.software.ibm.com/aixsupport/

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.

Linux

This bug was fixed in Linux NetKit 0.08 which is shipped with all reasonably up to date Linux distributions. Linux users using NetKit 0.07 or earlier should upgrade to NetKit 0.09. NetKit 0.09 has fixed other bugs and it is strongly recommended Linux users upgrade from NetKit 0.08 to NetKit 0.09. This is available from

ftp://ftp.uk.linux.org/pub/linux/Networking/base/NetKit-0.09.tar.gz

Some vendors have opted to issue NetKit 0.08 with additional fixes rather than 0.09. Consult your vendor for detailed information.

The Linux community would like to thank David A Holland for his continuing work on Linux network security.

NEC Corporation

UX/4800	Vulnerable for all versions.
EWS-UX/V(Rel4.2MP)	Vulnerable for all versions.
EWS-UX/V(Rel4.2)	Vulnerable for all versions.
UP-UX/V(Rel4.2MP)	Vulnerable for all versions.

Patches for these vulnerabilities are in progress.
Contacts for further information by e-mail:
UX48-security-support@nec.co.jp

The Santa Cruz Operation, Inc. (SCO)

SCO is investigating the problem with talkd and will provide updated information for this advisory as it becomes available. At this time SCO recommends disabling talkd on your SCO system as described herein.

Silicon Graphics Inc. (SGI)

For additional information refer to the Silicon Graphics Inc. Security Advisory Number 19970701-01-PX.
The SGI anonymous FTP site is sgigate.sgi.com (204.94.209.1) or its mirror, ftp.sgi.com. Security information and patches can be found in the ~ftp/security and ~ftp/patches directories, respectfully.

Solbourne (Grumman System Support)

We have examined the Solbourne implementation and found that it is vulnerable. Solbourne distributed the Sun application under license. We will distribute a Solbourne patch based on the Sun patch when it becomes available. For the latest information on our patches go to http://ftp.nts.gssc.com/solbourne.html

The workaround of disabling in.talkd can be used.
as root:

```
/etc/inetd.conf - comment out the talkd program
# ps -aux | grep inetd | grep -v grep
# kill -HUP {inetd PID listed in output of last command}
```

Sun Microsystems, Inc.

For additional information refer to the Sun Microsystems,
Inc. Security Bulletin Number #00147.
Patches are available to all Sun customers via World Wide Web at:

ftp://sunsolve1.sun.com/pub/patches/patches.html

Customers with Sun support contracts can also obtain patches from local Sun answer centers and SunSITEs worldwide.

Sun security bulletins are available via World Wide Web at:

http://sunsolve1.sun.com/sunsolve/secbulletins

Copyright 1997 Carnegie Mellon University.

Revision History

September 26, 1997 Updated copyright statement
July 28, 1997 Appendix A - updated patch information for Silicon Graphics,
Inc. and Sun Microsystems, Inc.
May 8, 1997 Appendix A - updated patch information for Hewlett-Packard.
Feb. 7, 1997 Appendix A - added an entry for Cisco Systems.