CERT Advisory CA-1999-11 Four Vulnerabilities in the Common Desktop Environment

Original release date: September 13, 1999
Last revised: March 02, 2000
Updated vendor information for Sun Microsystems, Inc.
Source: CERT/CC

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

Systems Affected

- Systems running the Common Desktop Environment (CDE)

I. Description

Multiple vulnerabilities have been identified in some distributions of the Common Desktop Environment (CDE). These vulnerabilities are different from those discussed in CA-98.02. We recommend that you install appropriate vendor patches as soon as possible (see Section III below). Until you can do so, we encourage you to disable or uninstall vulnerable copies of the CDE package. Note that disabling these programs will severely affect the utility of the CDE environment.

At this time, the CERT/CC has not received any reports of these vulnerabilities being exploited by intruders.

Vulnerability #1: ToolTalk *ttsession* uses weak RPC authentication mechanism

The ToolTalk messaging server *ttsession* allows independent applications to communicate without having direct knowledge of each other. Applications can communicate through an associated *ttsession* which delivers messages via RPC calls between interested agents.

On many systems, *ttsession* uses AUTH_UNIX authentication (a client-based security option) by default. When messages are received, *ttsession* uses certain environment variables supplied by the client to determine how the message is handled. Because of this, the *ttsession* process can be manipulated to execute unauthorized arbitrary programs with the privileges of the running ttsession.

Vulnerability #2: CDE *dtspcd* relies on file-system based authentication

The network daemon *dtspcd* (a CDE desktop subprocess control program) accepts CDE requests from clients to execute commands and launch applications remotely.

When a client makes a request, the *dtspcd* daemon asks the client to create a file that has a predictable name so that the daemon can authenticate the request. If a local user can manipulate the files used for authentication, then that user can craft arbitrary commands that may run as root.

Vulnerability #3: CDE *dtaction* buffer overflow

The *dtaction* utility allows applications or shell scripts that otherwise are not connected into the CDE development environment, to request that CDE actions be performed.

A buffer overflow can occur in some implementations of *dtaction* when a username argument greater than 1024 bytes is used.

Vulnerability #4: CDE ToolTalk shared library buffer overflow in TT_SESSION

There is a vulnerability in some implementations of the ToolTalk shared library which allows the TT_SESSION environment variable buffer to overflow. A setuid root program using a vulnerable ToolTalk library, such as *dtsession*, can be exploited to run arbitrary code as root.

II. Impact

Vulnerability #1: ToolTalk *ttsession* uses weak RPC authentication mechanism

A local or remote user may be able to use this vulnerability to run commands on a vulnerable system with the same privileges of the attacked *ttsession*. For this attack to work, a *ttsession* must be actively running on the system attacked. The *ttsession* daemon is started whenever a user logs in using the CDE desktop, or upon interaction with CDE at some future point.

Vulnerability #2: CDE *dtspcd* relies on file-system based authentication

A vulnerable *dtspcd* may allow a local user to run arbitrary commands as root.

Vulnerability #3: CDE *dtaction* buffer overflow

A local user may be able to exploit this vulnerability to execute arbitrary code with root privileges.

Vulnerability #4: CDE ToolTalk shared library buffer overflow in TT_SESSION

A local user may be able to exploit this vulnerability to execute arbitrary code with root privileges.

III. Solution

Install appropriate patches from your vendor

We recommend installing vendor patches as soon as possible and disabling the vulnerable programs until you can do so (or uninstalling the entire CDE package if not needed). Note that disabling these programs will severely affect the utility of the CDE environment.

Appendix A contains information provided by vendors for this advisory. We will update the appendix as we receive more information. If you do not see your vendor's name, the CERT/CC did not hear from that vendor. Please contact your vendor directly.

Appendix A. Vendor Information

Compaq Computer Corporation

Problem #1

CDE ToolTalk session daemon & ToolTalk shared library overflow

This potential security problem has been resolved and a patch for this problem has been made available for Tru64 UNIX V4.0D, V4.0E, V4.0F and V5.0.

This patch can be installed on:

```
V4.0D-F, all patch kits
V5.0, all patch kits
```

*This solution will be included in a future distributed release of Compaq's Tru64/ DIGITAL UNIX.

This patch may be obtained from the World Wide Web at the following FTP address:

http://www.service.digital.com/patches

The patch file name is **SSRT0617_ttsession.tar.Z**

Problem #2

Compaq's Tru64/DIGITAL UNIX is not vulnerable.

Problem #3

CDE dtaction buffer overflow

This potential security problem has been resolved and a patch for this problem has been made available for Tru64 UNIX V4.0D, V4.0E and V4.0F.

This patch can be installed on:

```
V4.0D Patch kit BL11 or BL12
V4.0E Patch kit BL1 or BL12
V4.0F Patch kit BL1
```

*This solution will be included in a future distributed release of Compaq's Tru64/ DIGITAL UNIX.

This patch may be obtained from the World Wide Web at the following FTP address:

http://www.service.digital.com/patches

The patch file name is **SSRT0615U_dtaction.tar.Z**

Problem #4

CDE ToolTalk shared library overflow

See solution fix described in in Problem #1. Data General

DG/UX is not subject to any of these vulnerabilities. **Fujitsu**

Fujitsu's UXP/V operating system is not vulnerable to any of these vulnerabilities. **Hewlett-Packard Company**

HP-9000 Series 700/800 HP-UX releases 10.X and 11.0 systems with CDE patches previously recommended in HP Security Bulletins are not vulnerable to vulnerabilities #2, #3, and #4.

All HP-UX 10.X and 11.0 systems running CDE are vulnerable to vulnerability #1.

Patches are in progress. **IBM Corporation**

All releases of AIX version 4 are vulnerable to vulnerabilities #1, #3, and #4. AIX is not vulnerable to #2. The following APARs will be available soon:

```
AIX 4.1.x:  IY03125  IY03847
AIX 4.2.x:  IY03105  IY03848
AIX 4.3.x:  IY02944  IY03849
```

Customers that do not require the CDE desktop functionality can disable CDE by restricting access to the CDE daemons and removing the **dt** entry from /etc/inittab. Run the following commands as root to disable CDE:

```
# /usr/dt/bin/dtconfig -d
# chsubserver -d -v dtspc
# chsubserver -d -v ttdbserver
# chsubserver -d -v cmsd
# chown root.system /usr/dt/bin/*
# chmod 0 /usr/dt/bin/*
```

For customers that require the CDE desktop functionality, a temporary fix is available via anonymous ftp from:

ftp://aix.software.ibm.com/aix/efixes/security/cdecert.tar.Z

```
Filename        sum             md5
================================================================
dtaction_4.1    32885    18     82af470bbbd334b240e874ff6745d8ca
dtaction_4.2    52162    18     b10f21abf55afc461882183fbd30e602
dtaction_4.3    56550    19     6bde84b975db2506ab0cbf9906c275ed
libtt.a_4.1     29234  2132     f5d5a59956deb8b1e8b3a14e94507152
libtt.a_4.2     21934  2132     73f32a73873caff06057db17552b8560
libtt.a_4.3     12154  2118     b0d14b9fe4a483333d64d7fd695f084d
ttauth          56348    31     495828ea74ec4c8f012efc2a9e6fa731
ttsession_4.1   19528   337     bfac4a06b90cbccc0cd494a44bd0ebc9
ttsession_4.2   46431   338     05949a483c4e390403055ff6961b0816
ttsession_4.3   54031   339     e1338b3167c7edf899a33520a3adb060
```

NOTE - This temporary fix has not been fully regression tested. Use the following steps (as root) to install the temporary fix.

```
1. Uncompress and extract the fix.

   # uncompress < cdecert.tar.Z | tar xf -
   # cd cdecert

2. Replace the vulnerable executables with the temporary fix for
   your version of AIX.

   # (cd /usr/dt/lib && mv libtt.a libtt.a.before_security_fix)
   # (cd /usr/dt/bin && mv ttsession ttsession.before_security_fix)
   # (cd /usr/dt/bin && mv dtaction dtaction.before_security_fix)
   # chown root.system /usr/dt/lib/libtt.a.before_security_fix
   # chown root.system /usr/dt/bin/ttsession.before_security_fix
   # chown root.system /usr/dt/bin/dtaction.before_security_fix
   # chmod 0 /usr/dt/lib/libtt.a.before_security_fix
   # chmod 0 /usr/dt/bin/ttsession.before_security_fix
   # chmod 0 /usr/dt/bin/dtaction.before_security_fix
   # cp ./libtt.a_ /usr/dt/lib/libtt.a
   # cp ./ttsession_ /usr/dt/bin/ttsession
   # cp ./dtaction_ /usr/dt/bin/dtaction
   # cp ./ttauth /usr/dt/bin/ttauth
   # chmod 555 /usr/dt/lib/libtt.a
   # chmod 555 /usr/dt/bin/ttsession
   # chmod 555 /usr/dt/bin/dtaction
   # chmod 555 /usr/dt/bin/ttauth
```

IBM AIX APARs may be ordered using Electronic Fix Distribution (via the FixDist program), or from the IBM Support Center. For more information on FixDist, and to obtain fixes via the Internet, please reference

http://techsupport.services.ibm.com/support/rs6000.support/downloads

or send electronic mail to "aixserv@austin.ibm.com" with the word "FixDist" in the "Subject:" line. To facilitate ease of ordering all security related APARs for each AIX release, security fixes are periodically bundled into a cumulative APAR. For more information on these cumulative APARs including last update and list of individual fixes, send electronic mail to "aixserv@austin.ibm.com" with the word "subscribe Security_APARs" in the "Subject:" line. **Santa Cruz Operation, Inc.**

SCO is investigating these vulnerabilities on SCO UnixWare 7. Other SCO products (OpenServer 5.0.x, UnixWare 2.1.x, Open Server / Open Desktop 3.0 and CMW+) are not vulnerable as CDE is not a component of these releases.

SCO will make patches and status information available at

http://www.sco.com/security. **Silicon Graphics, Inc.**

SGI acknowledges the CDE vulnerabilities reported and is currently investigating. No further information is available at this time. As further information becomes available, additional advisories will be issued via the normal SGI security information distribution methods including the wiretap mailing list.

Until SGI has more definitive information to provide, customers are encouraged to assume all security vulnerabilities as exploitable and take appropriate steps according to local site security policies and requirements.

The SGI Security Headquarters Web page is accessible at the URL

http://www.sgi.com/Support/security/security.html **Sun Microsystems, Inc.**

Please see Sun Security Bulletin #00192: CDE and OpenWindows at

http://sunsolve.sun.com/pub-cgi/retrieve.pl?doctype=coll&doc=secbull/192&type=0&nav=sec.sba

---

The CERT Coordination Center would like to thank Job de Haas for reporting these vulnerabilities and working with the vendors to effect fixes. We would also like to thank Solutions Atlantic for their efforts in coordinating vendor solutions.

Revision History

```
Mar  02, 2000:        Updated vendor information for Sun Microsystems, Inc.
Oct  04, 1999:  Updated vendor information for Sun Microsystems, Inc.
Oct  01, 1999:  Added vendor information for Data General
Sep  13, 1999:  Initial release
```