CERT Advisory CA-2002-01 Exploitation of Vulnerability in CDE Subprocess Control Service

Original release date: January 14, 2002
Last revised: --
Source: CERT/CC

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

Systems Affected

- Systems running CDE

Overview

The CERT/CC has received credible reports of scanning and exploitation of Solaris systems running the CDE Subprocess Control Service buffer overflow vulnerability identified in
CA-2001-31 and discussed in VU#172583.

I. Description

Since
CA-2001-31 was originally released last November, the CERT/CC has received reports of scanning for dtspcd (6112/tcp). Just recently, however, we have received credible reports of an exploit for Solaris systems. Using network traces provided by The Honeynet Project, we have confirmed that the dtspcd vulnerability identified in CA-2001-31 and discussed in VU#172583 is actively being exploited.

The Common Desktop Environment (CDE) is an integrated graphical user interface that runs on UNIX and Linux operating systems. The CDE Subprocess Control Service (dtspcd) is a network daemon that accepts requests from clients to execute commands and launch applications remotely. On systems running CDE, dtspcd is spawned by the Internet services daemon (typically inetd or xinetd) in response to a CDE client request. dtspcd is typically configured to run on port 6112/tcp with root privileges.

There is a remotely exploitable buffer overflow vulnerability in a shared library that is used by dtspcd. During client negotiation, dtspcd accepts a length value and subsequent data from the client without performing adequate input validation. As a result, a malicious client can manipulate data sent to dtspcd and cause a buffer overflow, potentially executing code with root privileges. The overflow occurs in a fixed-size 4K buffer that is exploited by the contents of one of the attack packets. The signature can be found at bytes 0x3e-0x41 in the following attack packet from a tcpdump log (lines may wrap):

```
09:46:04.378306 10.10.10.1.3592 > 10.10.10.2.6112: P 1:1449(1448) ack 1 win 16060 <nop,nop,timestamp 463986683 4158792> (DF)
0x0000   4500 05dc a1ac 4000 3006 241c 0a0a 0a01        E.....@.0.$.....
0x0010   0a0a 0a02 0e08 17e0 fee2 c115 5f66 192f        ...f........_f./
0x0020   8018 3ebc e1e9 0000 0101 080a 1ba7 dffb        ..>.............
0x0030   003f 7548 3030 3030 3030 3032 3034 3130        .?uH000000020410
0x0040   3365 3030 3031 2020 3420 0000 0031 3000        3e0001..4....10.
0x0050   801c 4011 801c 4011 1080 0101 801c 4011        ..@...@.......@.
0x0060   801c 4011 801c 4011 801c 4011 801c 4011        ..@...@...@...@.
...
```

The value 0x103e in the ASCII (right) column above is interpreted by the server as the number of bytes in the packet to copy into the internal 4K (0x1000) buffer. Since 0x103e is greater than 0x1000, the last 0x3e bytes of the packet will overwrite memory after the end of the 4K buffer. This is the same compromise vector identified in VU#172583.

It is important to note that several Internet-enabled games may also use port 6112/tcp as a legitimate part of their normal operation, therefore, not all network activity involving this service may be malicious. Network administrators monitoring this type of activity may wish to verify whether probes of this type are actually attempts to exploit VU#172583.

Many common UNIX systems ship with CDE installed and enabled by default. To determine if your system is configured to run dtspcd, check for the following entries (lines may wrap):

in /etc/services

```
dtspc 6112/tcp
```

in /etc/inetd.conf

```
dtspc stream tcp nowait root /usr/dt/bin/dtspcd /usr/dt/bin/dtspcd
```

Any system that does not run the CDE Subprocess Control Service is not vulnerable to this problem.

II. Impact

An attacker can execute arbitrary code with root privileges.

III. Solution

Apply a patch

VU#172583 contains information from vendors who have provided information for this advisory. We will update the vulnerability note as we receive more information. If a vendor's name does not appear, then the CERT/CC did not hear from that vendor. Please contact your vendor directly.

Vendor information can be found in the "Systems Affected" section of VU#172583

> http://www.kb.cert.org/vuls/id/172583#systems

Limit access to vulnerable service

Until patches are available and can be applied, you may wish to limit or block access to the Subprocess Control Service from untrusted networks such as the Internet. Using a firewall or other packet-filtering technology, block or restrict access to the port used by the Subprocess Control Service. As noted above, dtspcd is typically configured to listen on port 6112/tcp. It may be possible to use TCP Wrapper or a similar technology to provide improved access control and logging functionality for dtspcd connections. Keep in mind that blocking ports at a network perimeter does not protect the vulnerable service from the internal network. It is important to understand your network configuration and service requirements before deciding what changes are appropriate.

TCP Wrapper is available from

> ftp://ftp.porcupine.org/pub/security/index.html

Disable vulnerable service

You may wish to consider disabling dtspcd by commenting out the appropriate entry in /etc/inetd.conf. As a best practice, the CERT/CC recommends disabling any services that are not explicitly required. As noted above, it is important to consider the consequences of such a change in your environment.

Appendix A. - References

1. http://www.kb.cert.org/vuls/id/172583
2. http://www.cert.org/advisories/CA-2001-31.html
3. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0803
4. http://xforce.iss.net/alerts/advise101.php
5. http://www.opengroup.org/cde/
6. http://www.opengroup.org/desktop/faq/

The CERT Coordination Center thanks The Honeynet Project for their assistance in providing network traces of the exploitation.

Authors: Allen Householder and Art Manion

Revision History

```
January 14, 2002:  Initial release
```