Vulnerability in Common Desktop Environment (CDE) (US-CERT Vulnerability Note VU#179804)

Advisory Original Release Date: June 29, 2004
Last Revised: June 29, 2004
Number: 04-18
Risk Level: Medium
Advisory Version: 1.1

Advisory Status: Final

Overview:

A "double-free" vulnerability in the CDE dtlogin program could allow a remote attacker to execute arbitrary code or cause a denial of service on a vulnerable system.

The Common Desktop Environment (CDE) is an integrated graphical user interface that runs on UNIX and Linux operating systems. The dtlogin program contains a "double-free" vulnerability that can be triggered by a specially crafted X Display Manager Control Protocol (XDMCP) packet.

Impact:

Depending on configuration, operating system, and platform architecture, an unauthenticated, remote attacker could execute arbitrary code, read sensitive information, or cause a denial of service.

A local or remote unprivileged user may be able to gain unauthorized root privileges or cause a denial of service due to a "double-free" vulnerability in the CDE login service dtlogin(1X) which can be triggered when parsing invalid X Display Manager Control Protocol (XDMCP) packets. If the dtlogin(1X) program is killed, users will be unable to login on any Sun Ray devices attached to the server, and the console will display the command line login prompt.

Recommended Actions:

The following Avaya products are susceptible to this vulnerability and the following actions are recommended:

Avaya product	Affected S/W Version	Actions
Avaya IR (Interactive Response)	All Versions	Disable XDMCP Service as described below.
Avaya CMS	All Versions	Disable XDMCP Service as described below.

Mitigating Actions:

Avaya recommends that customers follow mitigating recommendations described below (disabling XDMCP Service). A patch may be certified by Avaya at a later time.

Disabling XDMCP Service:

Furthermore, Avaya has found that the part of dtlogin that is vulnerable is the XDMCP network service. This service accepts requests from remote X-terminals which CMS and Avaya IR does not use and can be disabled. Disabling this part of dtlogin will not affect stand-alone workstations like CMS or Avaya IR.

To disable XDMCP, follow these steps:

From the command line run:

cp /usr/dt/config/Xconfig /etc/dt/config/Xconfig

vi /etc/dt/config/Xconfig

uncomment the line that reads

"# Dtlogin.requestPort: 0"

Restart the dtlogin server.

/etc/rc2.d/S99dtlogin stop

/etc/rc2.d/S99dtlogin start

Additional Information:

US-CERT: http://www.kb.cert.org/vuls/id/179804

Sun Microsystems:
http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F57539

See http://support.avaya.com/security for the latest version of this advisory.

Additional information may be available via the Avaya support website (http://support.avaya.com) and through your Avaya account representative. Customers can locate their support representative by visiting http://support.avaya.com/ or by calling 1-866-GO AVAYA (1-866-462-8292).

Avaya Global Services, as part of a security hardening service, offers quarterly and semi annual proactive security patch implementation for Avaya products. For details please contact Avaya Global Services at 1-866-832-0925, option 3.

Disclaimer: ALL INFORMATION IS BELIEVED TO BE CORRECT AT THE TIME OF PUBLICATION AND IS PROVIDED "AS IS". AVAYA INC., ON BEHALF ITSELF AND ITS SUBSIDIARIES AND AFFILIATES (HEREINAFTER COLLECTIVELY REFERRED TO

AS "AVAYA"), DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND FURTHERMORE, AVAYA MAKES NO REPRESENTATIONS OR WARRANTIES THAT THE STEPS RECOMMENDED WILL ELIMINATE SECURITY OR VIRUS THREATS TO CUSTOMERS' SYSTEMS. IN NO EVENT SHALL AVAYA BE LIABLE FOR ANY DAMAGES WHATSOEVER ARISING OUT OF OR IN CONNECTION WITH THE INFORMATION OR RECOMMENDED ACTIONS PROVIDED HEREIN, INCLUDING DIRECT, INDIRECT, CONSEQUENTIAL DAMAGES, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF AVAYA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE INFORMATION PROVIDED HERE DOES NOT AFFECT THE SUPPORT AGREEMENTS IN PLACE FOR AVAYA PRODUCTS. SUPPORT FOR AVAYA PRODUCTS CONTINUES TO BE EXECUTED AS PER EXISTING AGREEMENTS WITH AVAYA.

Revision History:

V 1.0 – June 29, 2004 - Initial statement issued.
V 1.0 – June 29, 2004 - Grammatical change.

Send information regarding any discovered security problems with Avaya products to either the contact noted in the product's documentation or securityalerts@avaya.com.