

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité du composant dtlogin de CDE

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2004-ALE-004>

Gestion du document

Référence	CERTA-2004-ALE-004-003
Titre	Vulnérabilité du composant dtlogin de CDE
Date de la première version	26 mars 2004
Date de la dernière version	05 août 2004
Source(s)	Bulletin de sécurité "Remote double-free vulnerability in dtlogin (CDE)" d'Immunity Note VU#179804 de US-CERT
Pièce(s) jointe(s)	Aucune

TAB. 1 – gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

Exécution de code arbitraire à distance.

2 Systèmes affectés

CDE (Common Desktop Environment) est une interface graphique livrée sur de nombreuses plates-formes Unix.

3 Résumé

Une vulnérabilité dans dtlogin peut être exploitée par un utilisateur mal intentionné afin d'exécuter du code arbitraire sur une plate-forme vulnérable.

4 Description

dtlogin est un des composants de CDE (Common Desktop Environment). Il permet de créer des sessions sur des plate-formes distantes via le protocole XDMCP (X Display Manager Control Protocol).

Au moyen d'une trame habilement constituée, un utilisateur mal intentionné peut exploiter une vulnérabilité présente dans le composant `dtlogin` afin d'exécuter du code arbitraire sur la plate-forme vulnérable.

5 Contournement provisoire

- Filtrer les trames à destination du port 177/UDP (utilisé par XDMCP) en provenance de l'Internet afin de limiter l'exploitation de cette vulnérabilité ;
- Désactiver l'utilisation de XDMCP en ajoutant la ligne suivante dans le fichier `/usr/dt/config/Xconfig: Dtlogin.requestPort: 0`

6 Solution

- Bulletin de sécurité "dtlogin improperly handles some XDMCP requests" d'IBM :
<http://www-1.ibm.com/services/continuity/recover1.nsf/mss/MSS-OAR-E01-2004.0545.1>
- Bulletin de sécurité HPSBTU01017 "HP Tru64 UNIX dtlogin and XDM potential unauthorized privileged access, denial of service" de Hewlett-Packard :
<http://www-1.ibm.com/services/continuity/recover1.nsf/mss/MSS-OAR-E01-2004.0552.1>
- Bulletin de sécurité HPSBUX01038 "HP-UX dtlogin unauthorized privileged access, denial of service" de Hewlett-Packard :
<http://www.itrc.hp.com>
- Bulletin de sécurité #57539 de Sun :
<http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F57539>
- Bulletin de sécurité de SGI 20040801-01-P du 01 août 2004 :
<ftp://patches.sgi.com/support/free/security/advisories/20040801-01-P.asc>

7 Documentation

- Bulletin de sécurité "Remote double-free vulnerability in dtlogin (CDE)" d'Immunity :
<http://www.immunitysec.com/downloads/dtlogin.sxw.pdf>
- Note VU#179804 de US-CERT :
<http://www.kb.cert.org/vuls/id/179804>
- Référence CVE CAN-2004-0368 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0368>

Gestion détaillée du document

26 mars 2004 version initiale.

29 avril 2004 ajout références aux avis de sécurité d'IBM et Hewlett-Packard.

14 mai 2004 ajout références aux avis de sécurité de Sun et Hewlett-Packard (HPSBUX01038).

05 août 2004 ajout référence au bulletin de sécurité SGI.