



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité
des systèmes d'information
CERTA

Paris, le 01 septembre 2004
N° CERTA-2004-AVI-285

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans l'agent de messagerie dtmail 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-AVI-285>

Gestion du document

Référence	CERTA-2004-AVI-285
Titre	Vulnérabilité dans l'agent de messagerie dtmail de CDE
Date de la première version	01 septembre 2004
Date de la dernière version	-
Source(s)	Bulletin de sécurité 57627 de SUN
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 ;
- élévation de privilèges ;
- atteinte à l'intégrité des données.

2 Systèmes affectés

La vulnérabilité affecte dtmail dans les versions 1.4 et 1.5 de CDE sur les plates-formes Solaris 8 et 9.

3 Résumé

Une vulnérabilité présente dans l'agent de messagerie dtmail de CDE permet à un individu mal intentionné d'élever ses privilèges.

4 Description

dtmail est un agent de messagerie (MUA) disponible dans l'environnement CDE (Common Desktop Environment).

Une vulnérabilité de type "chaîne de format" (format string) est présente dans l'une des fonctions utilisées par `dtmail`. Cette vulnérabilité peut être exploitée par un utilisateur local mal intentionné pour obtenir les droits du groupe `mail` et pouvoir lire, modifier ou détruire les méls des autres utilisateurs.

5 Contournement provisoire

Enlever le bit `gid` du binaire `dtmail` :

```
chmod 0555 /usr/dt/bin/dtmail
```

Attention, cette command rend impossible l'accès des boîtes aux lettres présentes sur les partages NFS.

6 Solution

Appliquer le correctif suivant la version affectée (cf. Documentation).

7 Documentation

Bulletin de sécurité 57627 de SUN :

<http://sunsolve.sun.com/search/document.do?assetkey=1-26-57627-1>

Gestion détaillée du document

01 septembre 2004 version initiale.