



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 16 décembre 2003
N° CERTA-2003-AVI-214

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de DameWare Mini Remote Control

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-2003-AVI-214>

Gestion du document

Référence	CERTA-2003-AVI-214
Titre	Vulnérabilité de DameWare Mini Remote Control
Date de la première version	16 décembre 2003
Date de la dernière version	–
Source(s)	–
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

- Déni de service ;
- exécution de code arbitraire à distance avec des privilèges élevés.

2 Systèmes affectés

Tout système Windows utilisant “DameWare Mini Remote Control” comme service.

3 Résumé

Une vulnérabilité, de type débordement de tampon, permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance sans authentification.

4 Description

“DameWare Mini Remote Control” est un utilitaire de prise en contrôle à distance d'un ordinateur Windows fonctionnant en mode client ou serveur. La vulnérabilité ci-dessus permet d'exécuter du code sur les hôtes censés être contrôlés à distance.

5 Contournement provisoire

Limiter l'accès au port d'écoute du service, 6129/tcp, à des adresses IP de confiance à l'aide de règles de filtrage.

6 Solution

Mettre à jour en version 3.73 au moins :
<http://www.dameware.com/download/>

7 Documentation

Avis original :
<http://sh0dan.org/files/dwmrcs372.txt>

Gestion détaillée du document

16 décembre 2003 version initiale.