



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 03 novembre 2000
N° CERTA-2000-AVI-068

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans un contrôle ActiveX de Windows 2000

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-2000-AVI-068>

Gestion du document

Référence	CERTA-2000-AVI-068
Titre	Vulnérabilité dans un contrôle ActiveX de Windows 2000
Date de la première version	03 novembre 2000
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft
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.

2 Systèmes affectés

- Windows 2000 Professional;
- Windows 2000 Server;
- Windows 2000 Advanced Server;
- Windows 2000 Datacenter Server.

3 Résumé

Un contrôle ActiveX de Windows 2000 permet à un utilisateur mal intentionné d'exécuter du code grâce à un débordement de mémoire dans ce contrôle.

4 Description

Une mauvaise implémentation du contrôle ActiveX *Microsoft System Monitor* permet à un utilisateur mal intentionné de construire habilement une page web ou un courrier électronique au format HTML, et d'exécuter du code arbitraire sur la machine de la victime qui le lit.

5 Contournement provisoire

Désactiver l'exécution des Contrôles ActiveX de votre navigateur et du logiciel de courrier électronique comme indiqué dans les bulletins CERTA-2000-AVI-002, CERTA-2000-ALE-001, CERTA-2000-ALE-002 et CERTA-2000-INF-002.

6 Solution

Appliquer le correctif de Microsoft :

<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=25532>

7 Documentation

Le bulletin de Sécurité Microsoft et sa FAQ :

<http://www.microsoft.com/technet/security/bulletin/ms00-085.asp>

<http://www.microsoft.com/technet/security/bulletin/fq00-085.asp>

Gestion détaillée du document

03 novembre 2000 version initiale.