



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 17 novembre 2000
N° CERTA-2000-AVI-072

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Microsoft Exchange 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-072>

Gestion du document

Référence	CERTA-2000-AVI-072
Titre	Vulnérabilité de Microsoft Exchange 2000
Date de la première version	17 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

Accès à des données non autorisées.

2 Systèmes affectés

Serveur de mail Microsoft Windows utilisant Exchange 2000 Revision A et précédentes (indiqué par le fait qu'il n'y a aucun nom de révision marqué sur le CD d'installation).

3 Résumé

Lors de son installation, MS Exchange 2000 crée un compte local. Si le serveur sur lequel est installé Exchange est un contrôleur de domaine Windows, ce compte utilisateur peut avoir accès à des données de tout le domaine en question.

4 Description

Lors de l'installation de Microsoft Exchange 2000 sur un système, le logiciel crée le compte local EUSR_EXSTOREEVENT qui a les privilèges d'un simple compte *utilisateur*. Ce compte a déjà accès localement à toutes les données du système qui lui sont autorisées.

Si le logiciel Exchange est installé sur un contrôleur de domaine Windows, ce compte a accès sur tout le domaine aux données accessibles par les utilisateurs du domaine.

Ce compte, auquel personne n'a accès normalement, peut être utilisé maladroitement, voire à mauvais escient, par un utilisateur qui en prendrait possession par n'importe quel moyen.

5 Contournement provisoire

Il est évident qu'il ne faut pas accumuler les services sur la même machine. En l'occurrence : ne pas installer Exchange sur un serveur qui est aussi contrôleur de domaine.

6 Solution

Appliquer le correctif Microsoft :

<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=25866>

Ou suivre les indications données dans l'article de la base de connaissances Microsoft :

<http://www.microsoft.com/technet/support//kb.asp?ID=278523>

7 Documentation

Le bulletin de sécurité Microsoft, sa FAQ et l'article de la base de connaissance :

<http://www.microsoft.com/technet/security/bulletin/MS00-088.asp>

<http://www.microsoft.com/technet/security/bulletin/fq00-088.asp>

<http://www.microsoft.com/technet/support//kb.asp?ID=278523>

Gestion détaillée du document

17 novembre 2000 version initiale.