



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 10 mars 2009
N° CERTA-2009-AVI-092

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le composant d'authentification Secure Channel de Microsoft Windows

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-2009-AVI-092>

Gestion du document

Référence	CERTA-2009-AVI-092
Titre	Vulnérabilité dans le composant d'authentification Secure Channel de Microsoft Windows
Date de la première version	10 mars 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS09-007 du 10 mars 2009
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

Contournement de la politique de sécurité.

2 Systèmes affectés

- Microsoft Windows 2000 Service Pack 4 ;
- Microsoft Windows XP Service Pack 2 et 3 ;
- Microsoft Windows XP professional x64 Edition et x64 Edition Service Pack 2 ;
- Microsoft Windows Server 2003 Service Pack 1 et 2, y compris les systèmes à base d'Itanium ;
- Microsoft Windows Vista et Service Pack 1 ;
- Microsoft Windows Vista x64 Edition et Service Pack 1 ;
- Microsoft Windows Server 2008 32-bit, x64 et à base d'Itanium.

3 Résumé

Une vulnérabilité dans le composant d'authentification SChannel de Microsoft Windows permet à un utilisateur malveillant d'usurper une identité afin de se connecter à un serveur.

4 Description

Une vulnérabilité dans le composant d'authentification SChannel peut être exploitée par un utilisateur malintentionné, ayant obtenu au préalable un certificat d'authentification, afin de se connecter à un serveur distant sans pour autant être en possession de la clé privée associée.

5 Solution

Se référer au bulletin de sécurité MS09-007 de Microsoft pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS09-007 du 10 mars 2009 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS09-007.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS09-007.msp>
- Référence CVE CVE-2009-0085 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0085>

Gestion détaillée du document

10 mars 2009 version initiale.