Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 11 juillet 2007
N° CERTA-2007-AVI-293

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du pare-feu Microsoft Vista

Gestion du document

Référence	CERTA-2007-AVI-293
Titre	Vulnérabilité du pare-feu Microsoft Vista
Date de la première version	11 juillet 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS07-038 du 10 juillet 2007
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 ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- Microsoft Windows Vista ;
- Microsoft Windows Vista x64 Edition.

3 Résumé

Une vulnérabilité a été identifiée dans le comportement du pare-feu de Microsoft Vista lié à l'interface Teredo. L'exploitation de celle-ci permettrait à une personne distante d'activer l'interface et de récupérer les informations nécessaires pour initier de nouvelles connexions avec le système vulnérable.

4 Description

Teredo est un protocole d'encapsulation permettant à une machine isolée de communiquer en IPv6 dans un environnement IPv4. Ce dernier est détaillé dans la note d'information CERTA-2006-INF-004.

Le pare-feu de Microsoft Vista ne filtre pas correctement le trafic à l'intention de l'interface dédiée à Teredo. Cette vulnérabilité s'applique pour toute machine dans un réseau, même exploitant des techniques de translation d'adresses (NAT).

Une personne distante peut ainsi activer cette interface et récupérer les informations nécessaires pour initier de nouvelles connexions avec le système vulnérable.

5 Solution

Se référer au bulletin de sécurité MS07-038 de Microsoft pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS07-038 du 10 juillet 2007 :
  http://www.microsoft.com/france/technet/security/Bulletin/MS07-038.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS07-038.mspx
- Référence CVE CVE-2007-3038 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3038
- Note d'information CERTA-2006-INF-004, « Migration IPv6 : enjeux de sécurité » :
  http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-004/

Gestion détaillée du document

11 juillet 2007 version initiale.