Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 06 juillet 2004
N° CERTA-2004-AVI-226

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de WinGate

Gestion du document

Référence	CERTA-2004-AVI-226
Titre	Vulnérabilité de WinGate
Date de la première version	06 juillet 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité iDEFENSE du 01 juillet 2004
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 ;
- lecture de fichiers arbitraires.

2 Systèmes affectés

- Pour WinGate série 5 : WinGate 5.2.3 build 901 et versions antérieures ;
- pour WinGate série 6 : WinGate 6.0 beta 2 build 942 et versions antérieures.

3 Résumé

Deux vulnérabilités dans WinGate permettent à un utilisateur mal intentionné de lire n'importe quel fichier.

4 Description

WinGate est un serveur mandataire pour plate-forme Microsoft Windows.
Deux vulnérabilités dans WinGate permettent à un utilisateur mal intentionné, via une URL habilement construite, de lire n'importe quel fichier sur la plate-forme où réside WinGate.

5 Contournement provisoire

Désactiver le serveur mandataire ou restreindre l'accès à des hôtes de confiance.

6 Solution

- Pour WinGate série 6, installer la version 6.0 RC1 (build 963) ;
- pour WinGate série 5, aucun correctif de disponible à ce jour.

WinGate est téléchargeable à l'adresse Internet suivante :
http://www.wingate.com/download.php

7 Documentation

- Site Internet de WinGate :
  http://www.wingate.com/product-wingate.php
- Bulletin de sécurité iDEFENSE du 01 juillet 2004 :
  http://www.idefense.com/application/poi/display?id=113
- Référence CVE CAN-2004-0577 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0577
- Référence CVE CAN-2004-0578 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0578

Gestion détaillée du document

06 juillet 2004 version initiale.