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 juin 2009
N° CERTA-2009-AVI-236

**Affaire suivie par :**
CERTA

# AVIS DU CERTA

## Objet : Multiples vulnérabilités de l'antivirus Norman



## Gestion du document

| | |
|---|---|
| Référence | CERTA-2009-AVI-236 |
| Titre | Multiples vulnérabilités de l'antivirus Norman |
| Date de la première version | 17 juin 2009 |
| Date de la dernière version | – |
| Source(s) | Bulletin de sécurité Norman du 8 juin 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

- Norman Endpoint Protection 7.x ;
- Norman Network Protection 3.x ;
- Norman Security Suite 7.x ;
- Norman Virus Control 5.x pour Windows ;
- Norman Virus Control 5.x pour Domino ;
- Norman Virus Control 5.x pour Exchange 5.5 et 2000 ;
- Norman Virus Control 5.x pour Firewall-1 ;
- Norman Virus Control 5.x pour IIS ;
- Norman Virus Control 5.x pour Linux ;
- Norman Virus Control 5.x pour MimeSweeper.

# 3 Résumé

Deux vulnérabilités ont été découvertes dans les produits Norman. L'exploitation de ces vulnérabilités permet de contourner la politique de filtrage.

# 4 Description

Deux vulnérabilités ont été découvertes dans les produits antivirus Norman :

– la première vulnérabilité résulte d'un mauvais traitement des fichiers au format `rar3` ;

– la seconde vulnérabilité résulte d'un mauvais traitement des fichiers au format `cab`.

L'exploitation de ces vulnérabilités permet à un attaquant, via un fichier spécialement construit, de contourner la politique de filtrage mise en place par l'antivirus.

# 5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

# 6 Documentation

– Bulletin de sécurité Norman du 08 juin 2009 :
http://www.norman.com/support/security_bulletins/69333/en

# Gestion détaillée du document

**17 juin 2009** version initiale.