



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 05 mai 2006
N° CERTA-2006-AVI-185

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de l'outil de surveillance réseau Nagios

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-2006-AVI-185>

Gestion du document

Référence	CERTA-2006-AVI-185
Titre	Vulnérabilité de l'outil de surveillance réseau Nagios
Date de la première version	05 mai 2006
Date de la dernière version	–
Source(s)	
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

Déni de service à distance.

2 Systèmes affectés

Nagios en versions sources :

- 1.x, jusqu'à 1.3 ;
- 2.x, jusqu'à 2.2.

3 Résumé

Une mauvaise gestion de l'entête HTTP des requêtes POST peut être exploitée pour provoquer une écriture hors tampon qui conduira, au moins, à l'arrêt du service.

4 Description

Nagios est un outil de surveillance réseau possédant une interface web de consultation. Une erreur dans la gestion des requêtes peut provoquer l'arrêt du processus.

5 Contournement provisoire

Restreindre l'accès au service à des adresses IP de confiance.

6 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation) ou mettre à jour les sources en versions 1.4 ou 2.3 au moins.

7 Documentation

- Site internet de Nagios :
<http://www.nagios.org>

Gestion détaillée du document

05 mai 2006 version initiale.