Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 24 juin 2009
N° CERTA-2009-AVI-249

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Nagios

Gestion du document

Référence	CERTA-2009-AVI-249
Titre	Vulnérabilité dans Nagios
Date de la première version	24 juin 2009
Date de la dernière version	–
Source(s)	Annonce de mise à jour Nagios du 23 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

- Exécution de code arbitraire à distance ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- Nagios, pour les versions antérieures à 3.1.1.

3 Résumé

Une vulnérabilité a été identifiée dans l'outil d'administration Nagios. L'exploitation de cette dernière permet de contourner la politique de sécurité mise en place et d'exécuter des commandes arbitraires sur le système vulnérable.

4 Description

Une vulnérabilité a été identifiée dans l'outil d'administration Nagios. Le script `statuswml.cgi` ne manipule pas correctement les données fournies pour le paramètre `ping`.

L'exploitation de cette vulnérabilité permet de contourner la politique de sécurité mise en place et d'exécuter des commandes arbitraires sur le système vulnérable.

5 Solution

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

6 Documentation

- Note de changement de version Nagios mise à jour le 23 juin 2009 :
  http://www.nagios.org/development/history/core-3x/
- Note de suivi de bogue Nagios 15 du 29 mai 2009 :
  http://tracker.nagios.org/view.php?id=15
- Site de téléchargement Nagios :
  http://www.nagios.org/download

Gestion détaillée du document

24 juin 2009 version initiale.