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 mai 2006
N° CERTA-2006-AVI-199-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de l'outil Nagios

Gestion du document

Référence	CERTA-2006-AVI-199-001
Titre	Vulnérabilité de l'outil Nagios
Date de la première version	16 mai 2006
Date de la dernière version	24 mai 2006
Source(s)	Bulletin de mise à jour Nagios
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 ;
- déni de service à distance.

2 Systèmes affectés

- Nagios versions antérieures à la version 1.4.1 ;
- Nagios versions antérieures à la version 2.3.1 ;

3 Description

Deux vulnérabilités de type débordement de variable ont été découvertes dans Nagios. Ces vulnérabilités peuvent être exploitées par un utilisateur distant par le biais d'une entête HTTP spécialement conçue.

L'exploitation de cette vulnérabilité permet d'effectuer un déni de service et/ou une compromission de la machine à distance.

4 Solution

Les versions sources 1.4.1 et 2.3.1 corrigent cette vulnérabilité (cf. section Documentation).

5 Documentation

- Bulletin de mise à jour Nagios :
  http://www.nagios.org/development/changelog.php
- Bulletin de sécurité Debian DSA 1072 du 22 mai 2006 :
  http://www.debian.org/security/2006/dsa-1072
- Bulletin de sécurité Gentoo GLSA-200605-07 du 16 mai 2006 :
  http://www.gentoo.org/security/en/glsa/glsa-200605-07.xml
- Bulletin de sécurité SUSE SuSE-SA:2006:005 du 19 mai 2006 (ne prend pas en compte CAN-2006-2489) :
  http://www.novell.com/linux/security/advisories/2006_05_19.html
- Bulletin de sécurité Ubuntu USN-282-1 du 08 mai 2006 (ne prend pas en compte CAN-2006-2489) :
  http://www.ubuntulinux.org/usn/usn-282-1
- Référence CVE CAN-2006-2162 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-2162
- Référence CVE CAN-2006-2489 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-2489

Gestion détaillée du document

16 mai 2006 version initiale ;

24 mai 2006 deux vulnérabilité du même type au lieu d'une ; ajout des références CVE correspondantes, ajout des bulletins de sécurité Ubuntu, Debian, Gentoo et SUSE.