

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans 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-2013-AVI-066>

Gestion du document

Référence	CERTA-2013-AVI-066
Titre	Multiples vulnérabilités dans Nagios
Date de la première version	28 janvier 2013
Date de la dernière version	–
Source(s)	Bulletin de sécurité Nagios du 12 janvier 2013
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

Versions antérieures à Nagios 3.4.4

3 Résumé

De multiples vulnérabilités ont été corrigées dans Nagios. La plus critique concerne un débordement de mémoire tampon pouvant mener un utilisateur malintentionné à exécuter du code arbitraire à distance.

4 Solution

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

5 Documentation

- Bulletin de sécurité Nagios du 12 janvier 2013 :
<http://www.nagios.org/projects/nagioscore/history/core-3x>
- Référence CVE CVE-2012-6096 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-6096>

Gestion détaillée du document

28 janvier 2013 version initiale.