

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans nginx

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-2011-AVI-648>

Gestion du document

Référence	CERTA-2011-AVI-648
Titre	Vulnérabilité dans nginx
Date de la première version	18 novembre 2011
Date de la dernière version	–
Source(s)	Notes de version nginx 1.0.10
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

nginx versions antérieures à 1.0.10.

3 Résumé

Une vulnérabilité a été corrigée dans nginx. Cette vulnérabilité peut être utilisée à distance pour provoquer un déni de service et potentiellement de l'exécution de code arbitraire.

4 Description

Une vulnérabilité de type corruption de mémoire a été corrigée dans la façon dont nginx résout des noms de domaine. Cette vulnérabilité peut être utilisée par une personne malveillante distante pour provoquer un déni de service et potentiellement exécuter du code arbitraire.

5 Solution

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

6 Documentation

- Notes de version nginx 1.0.10 :
<http://nginx.org/en/CHANGES-1.0>

Gestion détaillée du document

18 novembre 2011 version initiale.