



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 avril 2012
N° CERTA-2012-AVI-213

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-2012-AVI-213>

Gestion du document

Référence	CERTA-2012-AVI-213
Titre	Vulnérabilité dans nginx
Date de la première version	13 avril 2012
Date de la dernière version	–
Source	
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.

2 Systèmes affectés

Serveur HTTP nginx
– 1.1.3 à 1.1.18 ;
– 1.0.7 à 1.0.14.

3 Résumé

Le serveur nginx pour lequel le module `ngx_http_mp4_module` est activé et la directive MP4 positionnée présente une vulnérabilité permettant à un attaquant d'exécuter du code arbitraire au moyen d'un fichier MP4 spécialement construit.

4 Solution

Les versions 1.1.19 et 1.0.15 de nginx corrigent cette vulnérabilité.
Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

5 Documentation

- Bulletin de sécurité nginx du 12 avril 2012 :
http://nginx.org/en/security_advisories.html
- Référence CVE CVE-2012-2089 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2089>

Gestion détaillée du document

13 avril 2012 version initiale.