

Affaire suivie par :  
CERT-FR

## AVIS DU CERT-FR

**Objet : Vulnérabilité dans Nginx**

### Gestion du document

Référence	CERTFR-2017-AVI-211
Titre	Vulnérabilité dans Nginx
Date de la première version	12 juillet 2017
Date de la dernière version	–
Source(s)	Bulletin de sécurité Nginx du 11 juillet 2017
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(s)

– atteinte à la confidentialité des données

### 2 - Systèmes affectés

Nginx versions 0.5.6 à 1.13.2

### 3 - Résumé

Une vulnérabilité a été corrigée dans *Nginx*. Elle permet à un attaquant de provoquer une atteinte à la confidentialité des données.

### 4 - Solution

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

### 5 - Documentation

– Bulletin de sécurité Nginx du 11 juillet 2017  
<http://mailman.nginx.org/pipermail/nginx-announce/2017/000200.html>

– Référence CVE CVE-2017-7529  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7529>

## **Gestion détaillée du document**

**12 juillet 2017** version initiale.

---

Conditions d'utilisation de ce document : <http://cert.ssi.gouv.fr/cert-fr/apropos.html>  
Dernière version de ce document : <http://cert.ssi.gouv.fr/site/CERTFR-2017-AVI-211>

---