

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Vulnérabilité dans nginx

Gestion du document

Référence	CERTFR-2014-AVI-136
Titre	Vulnérabilité dans nginx
Date de la première version	20 mars 2014
Date de la dernière version	–
Source(s)	Bulletin de sécurité nginx du 18 mars 2014
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)

- exécution de code arbitraire à distance
- déni de service à distance
- atteinte à la confidentialité des données

2 - Systèmes affectés

- Nginx versions antérieures à 1.4.7
- Nginx versions antérieures à 1.5.12

3 - Résumé

Une vulnérabilité a été corrigée dans *nginx*. Elle permet à un attaquant de provoquer une exécution de code arbitraire à distance, un déni de service à distance et 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 18 mars 2014
http://nginx.org/en/security_advisories.html
- Référence CVE CVE-2014-0133
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0133>

Gestion détaillée du document

20 mars 2014 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-2014-AVI-136>
