Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 02 août 2016
N° CERTFR-2016-AVI-256

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans Nagios

Gestion du document

Référence	CERTFR-2016-AVI-256
Titre	Multiples vulnérabilités dans Nagios
Date de la première version	02 août 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité Nagios du 01 août 2016
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
- atteinte à l'intégrité des données
- injection de requêtes illégitimes par rebond

2 - Systèmes affectés

Nagios Core versions antérieures à 4.2.0

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *Nagios*. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, une atteinte à l'intégrité des données et une injection de requêtes illégitimes par rebond (CSRF).

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 01 août 2016
  https://www.nagios.org/projects/nagios-core/history/4x/
- Référence CVE CVE-2008-4796
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4796
- Référence CVE CVE-2013-4214
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-4214

Gestion détaillée du document

02 août 2016 version initiale.