

Affaire suivie par :  
CERT-FR

## AVIS DU CERT-FR

**Objet : Vulnérabilité dans Cisco CloudCenter Orchestrator Docker Engine**

### Gestion du document

Référence	CERTFR-2016-AVI-429
Titre	Vulnérabilité dans Cisco CloudCenter Orchestrator Docker Engine
Date de la première version	22 décembre 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco cisco-sa-20161221-cco du 21 décembre 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)

- élévation de privilèges

### 2 - Systèmes affectés

Cisco CloudCenter Orchestrator (CCO) sans le dernier correctif de sécurité

### 3 - Résumé

Une vulnérabilité a été corrigée dans *Cisco CloudCenter Orchestrator Docker Engine*. Elle permet à un attaquant de provoquer une élévation de privilèges.

### 4 - Solution

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

### 5 - Documentation

- Bulletin de sécurité Cisco cisco-sa-20161221-cco du 21 décembre 2016  
<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161221-cco>

– Référence CVE CVE-2016-9223  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9223>

## **Gestion détaillée du document**

**22 décembre 2016** 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-2016-AVI-429>

---