

Affaire suivie par :  
CERT-FR

## AVIS DU CERT-FR

### Objet : Multiples vulnérabilités dans les produits Cisco

### Gestion du document

Référence	CERTFR-2017-AVI-286
Titre	Multiples vulnérabilités dans les produits Cisco
Date de la première version	07 septembre 2017
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco cisco-sa-20170906-fnd du 06 septembre 2017 Bulletin de sécurité Cisco cisco-sa-20170906-stb du 06 septembre 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)

- déni de service à distance

### 2 - Systèmes affectés

- Cisco IoT Field Network Director versions antérieures à 4.0
- Cisco YesMaxTotal, YesMax HD, et YesQuattro STB sans le dernier correctif de sécurité

### 3 - Résumé

De multiples vulnérabilités ont été corrigées dans *les produits Cisco*. Elles permettent à un attaquant de provoquer un déni de service à distance.

### 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-20170906-fnd du 06 septembre 2017  
<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170906-fnd>
- Bulletin de sécurité Cisco cisco-sa-20170906-stb du 06 septembre 2017  
<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170906-stb>
- Référence CVE CVE-2017-6780  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6780>
- Référence CVE CVE-2017-6631  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6631>

## Gestion détaillée du document

07 septembre 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-286>

---