

Affaire suivie par :  
CERT-FR

## AVIS DU CERT-FR

**Objet : Multiples vulnérabilités dans les produits Cisco**

### Gestion du document

Référence	CERTFR-2016-AVI-024
Titre	Multiples vulnérabilités dans les produits Cisco
Date de la première version	20 janvier 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco cisco-sa-20160115-FireSIGHT du 15 janvier 2016 Bulletin de sécurité Cisco cisco-sa-20160115-fmc1 du 15 janvier 2016 Bulletin de sécurité Cisco cisco-sa-20160115-asa du 15 janvier 2016 Bulletin de sécurité Cisco cisco-sa-20160119-wsa du 19 janvier 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)

- contournement de la politique de sécurité
- atteinte à la confidentialité des données
- injection de code indirecte à distance

### 2 - Systèmes affectés

- Centre de gestion Cisco FireSIGHT s'exécutant sur les systèmes Cisco FireSIGHT versions 6.0.0 et 6.0.1
- Cisco ASA version 8.4
- Cisco Web Security Appliance (WSA) version 8.5.3-055
- Cisco Web Security Appliance (WSA) version 9.1.0-000
- Cisco Web Security Appliance (WSA) version 9.5.0-235

### 3 - Résumé

De multiples vulnérabilités ont été corrigées dans *les produits Cisco*. Elles permettent à un attaquant de provoquer un contournement de la politique de sécurité, une atteinte à la confidentialité des données et une injection de code indirecte à distance (XSS).

## 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-20160115-FireSIGHT du 15 janvier 2016  
<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160115-FireSIGHT>
- Bulletin de sécurité Cisco cisco-sa-20160115-fmc1 du 15 janvier 2016  
<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160115-fmc1>
- Bulletin de sécurité Cisco cisco-sa-20160115-asa du 15 janvier 2016  
<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160115-asa>
- Bulletin de sécurité Cisco cisco-sa-20160119-wsa du 19 janvier 2016  
<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160119-wsa>
- Référence CVE CVE-2016-1293  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1293>
- Référence CVE CVE-2016-1294  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1294>
- Référence CVE CVE-2016-1295  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1295>
- Référence CVE CVE-2016-1296  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1296>

## Gestion détaillée du document

**20 janvier 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-024>

---