

Affaire suivie par :  
CERT-FR

## AVIS DU CERT-FR

### Objet : Multiples vulnérabilités dans les produits Cisco

### Gestion du document

Référence	CERTFR-2016-AVI-111
Titre	Multiples vulnérabilités dans les produits Cisco
Date de la première version	31 mars 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco cisco-sa-20160330-fp du 30 mars 2016 Bulletin de sécurité Cisco cisco-sa-20160328-ucdm du 28 mars 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
- injection de code indirecte à distance

## 2 - Systèmes affectés

- Cisco Adaptive Security Appliance (ASA) séries 5500-X avec les services FirePOWER
- Cisco Advanced Malware Protection (AMP) pour réseaux, Appliances séries 7000
- Cisco Advanced Malware Protection (AMP) pour réseaux, Appliances séries 8000
- Cisco Appliances FirePOWER séries 7000
- Cisco Appliances FirePOWER séries 8000
- Cisco FirePOWER Threat Defense pour routeurs supportant le modèle IntServ (ISRs)
- Cisco Next Generation Intrusion Prevention System (NGIPS) pour Blue Coat X-Series
- Cisco Appliances Sourcefire 3D System
- Cisco Virtual Next-Generation Intrusion Prevention System (NGIPSv) pour VMware
- Dans les produits sus-cités, sont vulnérables ceux qui exécutent Cisco Firepower System Software, versions antérieures à 5.4.0.7, 5.4.1.6, ou 6.0.1
- Snort versions antérieures à 2.9.8.2
- Cisco Unified Communications Domain Manager version 8.1(1)

### 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 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-20160330-fp du 30 mars 2016  
<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160330-fp>
- Bulletin de sécurité Cisco cisco-sa-20160328-ucdm du 28 mars 2016  
<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160328-ucdm>
- Référence CVE CVE-2016-1345  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1345>
- Référence CVE CVE-2016-1314  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1314>

## Gestion détaillée du document

**31 mars 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-111>

---