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 14 janvier 2016
N° CERTFR-2016-AVI-021

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans les produits Cisco

Gestion du document

Référence	CERTFR-2016-AVI-021
Titre	Multiples vulnérabilités dans les produits Cisco
Date de la première version	14 janvier 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco cisco-sa-20160113-ise du 13 janvier 2016 Bulletin de sécurité Cisco cisco-sa-20160113-aironet du 13 janvier 2016 Bulletin de sécurité Cisco cisco-sa-20160113-air du 13 janvier 2016 Bulletin de sécurité Cisco cisco-sa-20160113-ise2 du 13 janvier 2016 Bulletin de sécurité Cisco cisco-sa-20160113-wlc du 13 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)

- déni de service à distance
- contournement de la politique de sécurité
- atteinte à la confidentialité des données

2 - Systèmes affectés

- Cisco ISE version 1.1
- Cisco ISE versions 1.2 antérieures au patch 17
- Cisco ISE versions 1.2.1 antérieures au patch 8
- Cisco ISE versions 1.3 antérieures au patch 5
- Cisco ISE versions 1.4 antérieures au patch 4
- points d'accès Cisco Aironet séries 1830e
- points d'accès Cisco Aironet séries 1830i
- points d'accès Cisco Aironet séries 1850e
- points d'accès Cisco Aironet séries 1850i
- Cisco ISE antéreur à la version 2.0

- Contrôleurs sans fil Cisco séries 2500
- Contrôleurs sans fil Cisco séries 5500
- Contrôleurs sans fil Cisco séries 8500
- Contrôleurs sans fil Cisco Flex séries 7500
- Contrôleurs sans fil Cisco virtuels

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, un contournement de la politique de sécurité et une atteinte à la confidentialité des données.

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-20160113-ise du 13 janvier 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160113-ise
- Référence CVE CVE-2015-6323
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6323
- Bulletin de sécurité Cisco cisco-sa-20160113-aironet du 13 janvier 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160113-aironet
- Référence CVE CVE-2015-6320
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6320
- Bulletin de sécurité Cisco cisco-sa-20160113-air du 13 janvier 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160113-air
- Référence CVE CVE-2015-6336
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6336
- Bulletin de sécurité Cisco cisco-sa-20160113-ise2 du 13 janvier 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160113-ise2
- Référence CVE CVE-2015-6317
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6317
- Bulletin de sécurité Cisco cisco-sa-20160113-wlc du 13 janvier 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160113-wlc
- Référence CVE CVE-2015-6314
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6314

Gestion détaillée du document

14 janvier 2016 version initiale.