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 24 mars 2016
N° CERTFR-2016-AVI-107

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans les produits Cisco

Gestion du document

Référence	CERTFR-2016-AVI-107
Titre	Multiples vulnérabilités dans les produits Cisco
Date de la première version	24 mars 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco cisco-sa-20160323-lisp du 23 mars 2016 Bulletin de sécurité Cisco cisco-sa-20160323-ios-ikev2 du 23 mars 2016 Bulletin de sécurité Cisco cisco-sa-20160323-dhcpv6 du 23 mars 2016 Bulletin de sécurité Cisco cisco-sa-20160323-smi du 23 mars 2016 Bulletin de sécurité Cisco cisco-sa-20160323-l4f du 23 mars 2016 Bulletin de sécurité Cisco cisco-sa-20160323-sip du 23 mars 2016 Bulletin de sécurité Cisco cisco-sa-20160323-ncs du 23 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)

- déni de service à distance
- atteinte à l'intégrité des données

2 - Systèmes affectés

- Commutateurs Cisco Catalyst séries 6500 et 6800 exécutant Cisco IOS avec LISP configuré
- Commutateurs Cisco Nexus séries 7000 et 7700 avec un module Gigabit Ethernet série M1 exécutant Cisco NX-OS avec LISP configuré
- Produits Cisco exécutant Cisco IOS ou IOS XE, voir sur le site du constructeur pour vérifier si votre système est vulnérable (lien fourni dans la rubrique Documentation)
- Produits Cisco exécutant Cisco IOS avec WAAS Express configuré sur une ou plusieurs interfaces sans fil, voir sur le site du constructeur pour vérifier si votre système est vulnérable (lien fourni dans la rubrique Documentation)
- Produits Cisco exécutant Cisco IOS, IOS XE ou Cisco Unified Communications Manager Software, configurés pour traiter les messages SIP , voir sur le site du constructeur pour vérifier si votre système est vulnérable (lien fourni dans la rubrique Documentation)

– Routeurs Cisco Network Convergence System séries 6000 exécutant Cisco IOS XR

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 et une atteinte à l'intégrité 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-20160323-lisp du 23 mars 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160323-lisp
- Bulletin de sécurité Cisco cisco-sa-20160323-ios-ikev2 du 23 mars 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160323-ios-ikev2
- Bulletin de sécurité Cisco cisco-sa-20160323-dhcpv6 du 23 mars 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160323-dhcpv6
- Bulletin de sécurité Cisco cisco-sa-20160323-smi du 23 mars 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160323-smi
- Bulletin de sécurité Cisco cisco-sa-20160323-l4f du 23 mars 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160323-l4f
- Bulletin de sécurité Cisco cisco-sa-20160323-sip du 23 mars 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160323-sip
- Bulletin de sécurité Cisco cisco-sa-20160323-ncs du 23 mars 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160323-ncs
- Référence CVE CVE-2016-1344
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1344
- Référence CVE CVE-2016-1347
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1347
- Référence CVE CVE-2016-1348
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1348
- Référence CVE CVE-2016-1349
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1349
- Référence CVE CVE-2016-1350
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1350
- Référence CVE CVE-2016-1351
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1351
- Référence CVE CVE-2016-1366
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1366

Gestion détaillée du document

24 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-107`