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 21 avril 2016
N° CERTFR-2016-AVI-140

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans les produits Cisco

Gestion du document

Référence	CERTFR-2016-AVI-140
Titre	Multiples vulnérabilités dans les produits Cisco
Date de la première version	21 avril 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité les produits Cisco cisco-sa-20160420-htrd du 20 avril 2016 Bulletin de sécurité les produits Cisco cisco-sa-20160420-libsrtp du 20 avril 2016 Bulletin de sécurité les produits Cisco cisco-sa-20160420-asa-dhcpv6 du 20 avril 2016 Bulletin de sécurité les produits Cisco cisco-sa-20160420-bdos du 20 avril 2016 Bulletin de sécurité les produits Cisco cisco-sa-20160420-wlc du 20 avril 2016 Bulletin de sécurité les produits Cisco cisco-sa-20160419-ios du 19 avril 2016 Bulletin de sécurité les produits Cisco cisco-sa-20160414-ucspe2 du 14 avril 2016 Bulletin de sécurité les produits Cisco cisco-sa-20160414-ucspe1 du 14 avril 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

2 - Systèmes affectés

- Cisco WLC versions antérieures à 8.0.132.0
- Produits Cisco exécutant libSRTP versions antérieures à 1.5.3. Voir sur le site du constructeur pour une liste exhaustive (cf. section Documentation, avis de sécurité cisco-sa-20160420-libsrtp)
- Cisco ASA 5500-X Series Next-Generation Firewalls versions 9.4 antérieures à 9.4.1
- Cisco ASA Services Module pour Cisco Catalyst 6500 Series Switches et Cisco 7600 Series Routers versions 9.4 antérieures à 9.4.1
- Cisco Adaptive Security Virtual Appliance (ASAv) versions 9.4 antérieures à 9.4.1
- Cisco IOS versions 15.5(3)M01 et antérieures
- Cisco IOS XE versions 3.2.0 à 3.18.0S
- Cisco Unified Computing System Platform Emulator

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 un contournement de la politique de sécurité.

4 - Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

5 - Documentation

- Bulletin de sécurité les produits Cisco cisco-sa-20160420-htrd du 20 avril 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160420-htrd
- Bulletin de sécurité les produits Cisco cisco-sa-20160420-libsrtp du 20 avril 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160420-libsrtp
- Bulletin de sécurité les produits Cisco cisco-sa-20160420-asa-dhcpv6 du 20 avril 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160420-asa-dhcpv6
- Bulletin de sécurité les produits Cisco cisco-sa-20160420-bdos du 20 avril 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160420-bdos
- Bulletin de sécurité les produits Cisco cisco-sa-20160420-wlc du 20 avril 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160420-wlc
- Bulletin de sécurité les produits Cisco cisco-sa-20160419-ios du 19 avril 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160419-ios
- Bulletin de sécurité les produits Cisco cisco-sa-20160414-ucspe2 du 14 avril 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160414-ucspe2
- Bulletin de sécurité les produits Cisco cisco-sa-20160414-ucspe1 du 14 avril 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160414-ucspe1
- Référence CVE CVE-2015-6360
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6360
- Référence CVE CVE-2016-1339
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1339
- Référence CVE CVE-2016-1340
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1340
- Référence CVE CVE-2016-1362
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1362
- Référence CVE CVE-2016-1363
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1363
- Référence CVE CVE-2016-1364
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1364
- Référence CVE CVE-2016-1367
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1367
- Référence CVE CVE-2016-1384
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1384

Gestion détaillée du document

21 avril 2016 version initiale.