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 02 septembre 2016
N° CERTFR-2016-AVI-291

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans les produits Cisco

Gestion du document

Référence	CERTFR-2016-AVI-291
Titre	Multiples vulnérabilités dans les produits Cisco
Date de la première version	02 septembre 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco cisco-sa-20160831-wlc-2 du 31 août 2016 Bulletin de sécurité Cisco cisco-sa-20160831-wlc-1 du 31 août 2016 Bulletin de sécurité Cisco cisco-sa-20160831-webex du 31 août 2016 Bulletin de sécurité Cisco cisco-sa-20160831-vmp du 31 août 2016 Bulletin de sécurité Cisco cisco-sa-20160831-sps3 du 31 août 2016 Bulletin de sécurité Cisco cisco-sa-20160831-sps2 du 31 août 2016 Bulletin de sécurité Cisco cisco-sa-20160831-sps1 du 31 août 2016 Bulletin de sécurité Cisco cisco-sa-20160831-sps du 31 août 2016 Bulletin de sécurité Cisco cisco-sa-20160831-spa du 31 août 2016 Bulletin de sécurité Cisco cisco-sa-20160831-meetings-player du 31 août 2016 Bulletin de sécurité Cisco cisco-sa-20160831-hcmf du 31 août 2016 Bulletin de sécurité Cisco cisco-sa-20160831-hcm du 31 août 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)

- exécution de code arbitraire à distance
- déni de service à distance
- contournement de la politique de sécurité
- atteinte à l'intégrité des données
- atteinte à la confidentialité des données
- injection de code indirecte à distance
- injection de requêtes illégitimes par rebond

2 - Systèmes affectés

- Cisco Wireless LAN Controller versions antérieures à 8.0.140.0

- Cisco WebEx Meetings Player versions antérieures à T29.10
- Cisco Virtual Media Packager (VMP) utilisant Media Origination System versions antérieures à 2.6
- Cisco Small Business 220 Series Smart Plus (Sx220) Switches versions 1.0.0.17, 1.0.0.18, ou 1.0.0.19 et qui ont la fonctionnalité SNMP activée
- SPA300 Series IP Phones utilisant une version de Cisco Small Business IP Phones inférieure à 7.5.7(6)
- SPA500 Series IP Phones utilisant une version de Cisco Small Business IP Phones inférieure à 7.5.7(6)
- SPA51x IP Phones utilisant une version de Cisco Small Business IP Phones inférieure à 7.5.7(6)
- Cisco Hosted Collaboration Mediation Fulfillment (HCM-F) versions antérieures à 10.6(3)

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *les produits Cisco*. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, 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 Cisco cisco-sa-20160831-wlc-2 du 31 août 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-wlc-2
- Bulletin de sécurité Cisco cisco-sa-20160831-wlc-1 du 31 août 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-wlc-1
- Bulletin de sécurité Cisco cisco-sa-20160831-webex du 31 août 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-webex
- Bulletin de sécurité Cisco cisco-sa-20160831-vmp du 31 août 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-vmp
- Bulletin de sécurité Cisco cisco-sa-20160831-sps3 du 31 août 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-sps3
- Bulletin de sécurité Cisco cisco-sa-20160831-sps2 du 31 août 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-sps2
- Bulletin de sécurité Cisco cisco-sa-20160831-sps1 du 31 août 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-sps1
- Bulletin de sécurité Cisco cisco-sa-20160831-sps du 31 août 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-sps
- Bulletin de sécurité Cisco cisco-sa-20160831-spa du 31 août 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-spa
- Bulletin de sécurité Cisco cisco-sa-20160831-meetings-player du 31 août 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-meetings-player
- Bulletin de sécurité Cisco cisco-sa-20160831-hcmf du 31 août 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-hcmf
- Bulletin de sécurité Cisco cisco-sa-20160831-hcm du 31 août 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-hcm

Gestion détaillée du document

02 septembre 2016 version initiale.