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 10 mars 2016
N° CERTFR-2016-AVI-093

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans les produits Cisco

Gestion du document

Référence	CERTFR-2016-AVI-093
Titre	Multiples vulnérabilités dans les produits Cisco
Date de la première version	10 mars 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco cisco-sa-20160309-cmre du 09 mars 2016 Bulletin de sécurité Cisco cisco-sa-20160309-cmdos du 09 mars 2016 Bulletin de sécurité Cisco cisco-sa-20160309-csc du 09 mars 2016 Bulletin de sécurité Cisco cisco-sa-20160309-rgid du 09 mars 2016 Bulletin de sécurité Cisco cisco-sa-20160302-cpi du 10 mars 2016 Bulletin de sécurité Cisco cisco-sa-20160309-vcs du 09 mars 2016 Bulletin de sécurité Cisco cisco-sa-20160302-cpi du 03 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)

- exécution de code arbitraire à distance
- déni de service à distance
- atteinte à la confidentialité des données

2 - Systèmes affectés

- Cisco Cable Modem avec Digital Voice Model DPC2203
- Cisco Cable Modem avec Digital Voice Model EPC2203
- Cisco Model DPQ3925 8x4 DOCSIS 3.0 Wireless Residential Gateway avec EDVA
- Cisco ASA 5500 Series CSC-SSM exécutant les versions 6.6 antérieures à 6.6.1164.0 ou n'intégrant pas le correctif de sécurité 1157
- Cisco DPC3941 Wireless Residential Gateway avec Digital Voice
- Cisco DPC3939B Wireless Residential Voice Gateway
- Cisco Prime LAN Management Solution (LMS)
- Cisco TelePresence Video Communication Server (VCS) exécutant les versions X8.5.2 ou X8.5.1
- Cisco Prime Infrastructure versions 2.2, 3.0, et 3.1(0.0)

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *les produits Cisco*. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, un déni de service à distance 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-20160309-cmre du 09 mars 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160309-cmre
- Bulletin de sécurité Cisco cisco-sa-20160309-cmdos du 09 mars 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160309-cmdos
- Bulletin de sécurité Cisco cisco-sa-20160309-csc du 09 mars 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160309-csc
- Bulletin de sécurité Cisco cisco-sa-20160309-rgid du 09 mars 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160309-rgid
- Bulletin de sécurité Cisco cisco-sa-20160310-prime-lms du 10 mars 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160310-prime-lms
- Bulletin de sécurité Cisco cisco-sa-20160309-vcs du 09 mars 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160309-vcs
- Bulletin de sécurité Cisco cisco-sa-20160302-cpi du 09 mars 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160302-cpi
- Référence CVE CVE-2016-1312
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1312
- Référence CVE CVE-2016-1325
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1325
- Référence CVE CVE-2016-1326
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1326
- Référence CVE CVE-2016-1327
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1327
- Référence CVE CVE-2016-1338
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1338
- Référence CVE CVE-2016-1358
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1358
- Référence CVE CVE-2016-1360
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1360

Gestion détaillée du document

10 mars 2016 version initiale.