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 08 juin 2017
N° CERTFR-2017-AVI-171

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans les produits Cisco

Gestion du document

Référence	CERTFR-2017-AVI-171
Titre	Multiples vulnérabilités dans les produits Cisco
Date de la première version	08 juin 2017
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco cisco-sa-20170607-tele du 07 juin 2017 Bulletin de sécurité Cisco cisco-sa-20170607-dcnm2 du 07 juin 2017 Bulletin de sécurité Cisco cisco-sa-20170607-dcnm1 du 07 juin 2017 Bulletin de sécurité Cisco cisco-sa-20170607-anyconnect du 07 juin 2017
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 la confidentialité des données
- élévation de privilèges

2 - Systèmes affectés

- TelePresence MX Series
- TelePresence Profile Series
- Telepresence SX Series
- TelePresence System Profile MXP Series
- Collaboration Desk Endpoints: DX Series
- TelePresence System EX Series
- TelePresence Integrator C Series
- Cisco Prime Data Center Network Manager (DCNM) versions logicielles antérieures à 10.2(1) pour Microsoft Windows, Linux, et les systèmes virtualisés

- Cisco Prime Data Center Network Manager (DCNM) versions logicielles 10.1(1) et 10.1(2) pour Microsoft Windows, Linux, et les systèmes virtualisés
- Cisco AnyConnect Secure Mobility Client pour Windows versions logicielles antérieures à 4.4.02034

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-20170607-tele du 07 juin 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170607-tele
- Bulletin de sécurité Cisco cisco-sa-20170607-dcnm2 du 07 juin 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170607-dcnm2
- Bulletin de sécurité Cisco cisco-sa-20170607-dcnm1 du 07 juin 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170607-dcnm1
- Bulletin de sécurité Cisco cisco-sa-20170607-anyconnect du 07 juin 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170607-anyconnect
- Référence CVE CVE-2017-6648
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6648
- Référence CVE CVE-2017-6640
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6640
- Référence CVE CVE-2017-6639
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6639
- Référence CVE CVE-2017-6638
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6638

Gestion détaillée du document

08 juin 2017 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-2017-AVI-171