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 03 novembre 2016
N° CERTFR-2016-AVI-366

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans les produits Cisco

Gestion du document

Référence	CERTFR-2016-AVI-366
Titre	Multiples vulnérabilités dans les produits Cisco
Date de la première version	03 novembre 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité les produits Cisco cisco-sa-20161102-cph du 02 novembre 2016 Bulletin de sécurité les produits Cisco cisco-sa-20161102-tl1 du 02 novembre 2016 Bulletin de sécurité les produits Cisco cisco-sa-20161102-cms du 02 novembre 2016 Bulletin de sécurité les produits Cisco cisco-sa-20161102-cms1 du 02 novembre 2016 Bulletin de sécurité les produits Cisco cisco-sa-20161102-asr du 02 novembre 2016 Bulletin de sécurité les produits Cisco cisco-sa-20161102-n9kapic du 02 novembre 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

2 - Systèmes affectés

- Cisco Prime Home versions antérieures à 5.1.1.7
- Cisco Prime Home versions antérieures à 5.2.2.3
- Cisco IOS XE versions antérieures à 3.18.2S s'exécutant sur les routeurs à services d'agrégation Cisco séries ASR 9000 (ASR902, ASR903, et ASR907)
- Acano Server versions antérieures à 1.8.17
- Acano Server versions 1.9.x antérieures à 1.9.5
- Cisco Meeting Server versions antérieures à 2.0.1
- Acano Meeting Apps versions antérieures à 1.8.35
- Acano Meeting Apps versions 1.9.x antérieures à 1.9.8

- StarOS versions 18.0 et ultérieures s'exécutant sur les routeurs Cisco séries ASR 5500 équipés de Data Processing Card 2 (DPC2)
- Cisco Nexus 9000 Series Leaf Switches (TOR) - ACI Mode et Cisco Application Policy Infrastructure Controller (APIC)

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 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-20161102-cph du 02 novembre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161102-cph
- Bulletin de sécurité les produits Cisco cisco-sa-20161102-tl1 du 02 novembre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161102-tl1
- Bulletin de sécurité les produits Cisco cisco-sa-20161102-cms du 02 novembre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161102-cms
- Bulletin de sécurité les produits Cisco cisco-sa-20161102-cms1 du 02 novembre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161102-cms1
- Bulletin de sécurité les produits Cisco cisco-sa-20161102-asr du 02 novembre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161102-asr
- Bulletin de sécurité les produits Cisco cisco-sa-20161102-n9kapic du 02 novembre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161102-n9kapic
- Référence CVE CVE-2016-6441
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6441
- Référence CVE CVE-2016-6447
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6447
- Référence CVE CVE-2016-6448
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6448
- Référence CVE CVE-2016-6452
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6452
- Référence CVE CVE-2016-6455
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6455
- Référence CVE CVE-2016-6457
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6457

Gestion détaillée du document

03 novembre 2016 version initiale.