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 18 mai 2017
N° CERTFR-2017-AVI-160

**Affaire suivie par :**
CERT-FR

# AVIS DU CERT-FR

**Objet : Multiples vulnérabilités dans les produits Cisco**

## Gestion du document

| | |
|---|---|
| Référence | CERTFR-2017-AVI-160 |
| Titre | Multiples vulnérabilités dans les produits Cisco |
| Date de la première version | 18 mai 2017 |
| Date de la dernière version | – |
| Source(s) | Bulletin de sécurité Cisco cisco-sa-20170517-pcp1 du 17 mai 2017<br>Bulletin de sécurité Cisco cisco-sa-20170517-pcp2 du 17 mai 2017<br>Bulletin de sécurité Cisco cisco-sa-20170517-telepresence-ix5000 du 17 mai 2017<br>Bulletin de sécurité Cisco cisco-sa-20170517-cps du 17 mai 2017<br>Bulletin de sécurité Cisco cisco-sa-20170517-fpwr du 17 mai 2017<br>Bulletin de sécurité Cisco cisco-sa-20170517-ie1000csrf du 17 mai 2017<br>Bulletin de sécurité Cisco cisco-sa-20170517-ise du 17 mai 2017<br>Bulletin de sécurité Cisco cisco-sa-20170517-nss du 17 mai 2017<br>Bulletin de sécurité Cisco cisco-sa-20170517-nss1 du 17 mai 2017<br>Bulletin de sécurité Cisco cisco-sa-20170517-pcp3 du 17 mai 2017<br>Bulletin de sécurité Cisco cisco-sa-20170517-pcp4 du 17 mai 2017<br>Bulletin de sécurité Cisco cisco-sa-20170517-pcp5 du 17 mai 2017<br>Bulletin de sécurité Cisco cisco-sa-20170517-rem1 du 17 mai 2017<br>Bulletin de sécurité Cisco cisco-sa-20170517-rem2 du 17 mai 2017<br>Bulletin de sécurité Cisco cisco-sa-20170517-rem3 du 17 mai 2017<br>Bulletin de sécurité Cisco cisco-sa-20170517-rem4 du 17 mai 2017<br>Bulletin de sécurité Cisco cisco-sa-20170517-rem5 du 17 mai 2017<br>Bulletin de sécurité Cisco cisco-sa-20170517-rem6 du 17 mai 2017<br>Bulletin de sécurité Cisco cisco-sa-20170517-rem7 du 17 mai 2017<br>Bulletin de sécurité Cisco cisco-sa-20170517-sip du 17 mai 2017<br>Bulletin de sécurité Cisco cisco-sa-20170517-ucm du 17 mai 2017<br>Bulletin de sécurité Cisco cisco-sa-20170517-ucsc du 17 mai 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 l'intégrité des données
- atteinte à la confidentialité des données
- élévation de privilèges
- injection de code indirecte à distance
- injection de requêtes illégitimes par rebond

## 2 - Systèmes affectés

- Cisco Prime Collaboration Provisioning versions antérieures à 12.1
- Cisco TelePresence IX5000 Series versions antérieures à 8.2.1
- Cisco Policy Suite versions antérieures à 11.1.0, 12.0.0 et 12.1.0
- Cisco FirePOWER System
- Commutateurs Ethernet Cisco Industrial séries 1000
- Cisco Identity Services Engine (ISE)
- Commutateurs Cisco Nexus séries 5000
- Cisco Remote Expert Manager
- Cisco IP Phone 8851
- Cisco Unified Communications Manager
- Cisco UCS C-Series Rack Servers

## 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-20170517-pcp1 du 17 mai 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-pcp1
- Bulletin de sécurité Cisco cisco-sa-20170517-pcp2 du 17 mai 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-pcp2
- Bulletin de sécurité Cisco cisco-sa-20170517-telepresence-ix5000 du 17 mai 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-telepresence-ix5000
- Bulletin de sécurité Cisco cisco-sa-20170517-cps du 17 mai 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-cps
- Bulletin de sécurité Cisco cisco-sa-20170517-fpwr du 17 mai 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-fpwr
- Bulletin de sécurité Cisco cisco-sa-20170517-ie1000csrf du 17 mai 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-ie1000csrf
- Bulletin de sécurité Cisco cisco-sa-20170517-ise du 17 mai 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-ise
- Bulletin de sécurité Cisco cisco-sa-20170517-nss du 17 mai 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-nss

- Bulletin de sécurité Cisco cisco-sa-20170517-nss1 du 17 mai 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-nss1
- Bulletin de sécurité Cisco cisco-sa-20170517-pcp3 du 17 mai 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-pcp3
- Bulletin de sécurité Cisco cisco-sa-20170517-pcp4 du 17 mai 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-pcp4
- Bulletin de sécurité Cisco cisco-sa-20170517-pcp5 du 17 mai 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-pcp5
- Bulletin de sécurité Cisco cisco-sa-20170517-rem1 du 17 mai 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-rem1
- Bulletin de sécurité Cisco cisco-sa-20170517-rem2 du 17 mai 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-rem2
- Bulletin de sécurité Cisco cisco-sa-20170517-rem3 du 17 mai 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-rem3
- Bulletin de sécurité Cisco cisco-sa-20170517-rem4 du 17 mai 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-rem4
- Bulletin de sécurité Cisco cisco-sa-20170517-rem5 du 17 mai 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-rem5
- Bulletin de sécurité Cisco cisco-sa-20170517-rem6 du 17 mai 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-rem6
- Bulletin de sécurité Cisco cisco-sa-20170517-rem7 du 17 mai 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-rem7
- Bulletin de sécurité Cisco cisco-sa-20170517-sip du 17 mai 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-sip
- Bulletin de sécurité Cisco cisco-sa-20170517-ucm du 17 mai 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-ucm
- Bulletin de sécurité Cisco cisco-sa-20170517-ucsc du 17 mai 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-ucsc
- Référence CVE CVE-2017-6621
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6621
- Référence CVE CVE-2017-6622
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6622
- Référence CVE CVE-2017-6623
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6623
- Référence CVE CVE-2017-6630
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6630
- Référence CVE CVE-2017-6632
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6632
- Référence CVE CVE-2017-6633
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6633
- Référence CVE CVE-2017-6634
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6634
- Référence CVE CVE-2017-6635
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6635
- Référence CVE CVE-2017-6636
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6636
- Référence CVE CVE-2017-6637
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6637
- Référence CVE CVE-2017-6641
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6641
- Référence CVE CVE-2017-6642
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6642
- Référence CVE CVE-2017-6643
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6643

- Référence CVE CVE-2017-6644
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6644
- Référence CVE CVE-2017-6645
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6645
- Référence CVE CVE-2017-6646
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6646
- Référence CVE CVE-2017-6647
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6647
- Référence CVE CVE-2017-6649
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6649
- Référence CVE CVE-2017-6650
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6650
- Référence CVE CVE-2017-6652
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6652
- Référence CVE CVE-2017-6653
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6653
- Référence CVE CVE-2017-6654
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6654

# Gestion détaillée du document

**18 mai 2017** version initiale.