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 04 février 2016
N° CERTFR-2016-AVI-047

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans les produits Cisco

Gestion du document

Référence	CERTFR-2016-AVI-047
Titre	Multiples vulnérabilités dans les produits Cisco
Date de la première version	04 février 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco cisco-sa-20160203-n9knci du 03 février 2016 Bulletin de sécurité Cisco cisco-sa-20160203-prsm du 03 février 2016 Bulletin de sécurité Cisco cisco-sa-20160203-apic du 03 février 2016 Bulletin de sécurité Cisco cisco-sa-20160203-ucm du 03 février 2016 Bulletin de sécurité Cisco cisco-sa-20160203-uc du 03 février 2016 Bulletin de sécurité Cisco cisco-sa-20160203-jgs du 03 février 2016 Bulletin de sécurité Cisco cisco-sa-20160202-wms du 02 février 2016 Bulletin de sécurité Cisco cisco-sa-20160202-fducce du 02 février 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)

- déni de service à distance
- contournement de la politique de sécurité
- atteinte à la confidentialité des données
- élévation de privilèges
- injection de code indirecte à distance

2 - Systèmes affectés

- Cisco Nexus 9000 Series ACI Mode Switches versions antérieures à 11.0(1c)
- Cisco ASA-CX Content-Aware Security et Cisco PRSM versions antérieures à 9.3.1.1(112)
- Cisco Application Policy Infrastructure Controllers versions antérieures à 1.0(3h) et 1.1(1j)
- Cisco Nexus 9000 Series ACI Mode Switches versions antérieures à 1.0(3h) et 1.1(1j)
- Cisco Unified Communications Manager version 10.5(2.13900.9)
- Cisco Unity Connection version 11.5(0.199)

- Cisco Jabber Guest Server version 10.6(8)
- Cisco WebEx Meetings Server version 2.5.1.5
- Cisco Finesse Desktop versions 10.5(1) et 11.0(1)
- Cisco Unified Contact Center Express version 10.6(1)

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *les produits Cisco*. Certaines d'entre elles permettent à un attaquant de provoquer un déni de service à distance, un contournement de la politique de sécurité 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-20160203-n9knci du 03 février 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160203-n9knci
- Bulletin de sécurité Cisco cisco-sa-20160203-prsm du 03 février 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160203-prsm
- Bulletin de sécurité Cisco cisco-sa-20160203-apic du 03 février 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160203-apic
- Bulletin de sécurité Cisco cisco-sa-20160203-ucm du 03 février 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160203-ucm
- Bulletin de sécurité Cisco cisco-sa-20160203-uc du 03 février 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160203-uc
- Bulletin de sécurité Cisco cisco-sa-20160203-jgs du 03 février 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160203-jgs
- Bulletin de sécurité Cisco cisco-sa-20160202-wms du 02 février 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160202-wms
- Bulletin de sécurité Cisco cisco-sa-20160202-fducce du 02 février 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160202-fducce
- Référence CVE CVE-2015-6398
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6398
- Référence CVE CVE-2016-1301
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1301
- Référence CVE CVE-2016-1302
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1302
- Référence CVE CVE-2016-1308
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1308
- Référence CVE CVE-2016-1310
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1310
- Référence CVE CVE-2016-1311
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1311
- Référence CVE CVE-2016-1309
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1309
- Référence CVE CVE-2016-1307
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1307

Gestion détaillée du document

04 février 2016 version initiale.