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 02 février 2016
N° CERTFR-2016-AVI-045

**Affaire suivie par :**
CERT-FR

# AVIS DU CERT-FR

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

## Gestion du document

| | |
|---|---|
| Référence | CERTFR-2016-AVI-045 |
| Titre | Multiples vulnérabilités dans les produits Cisco |
| Date de la première version | 02 février 2016 |
| Date de la dernière version | – |
| Source(s) | Bulletin de sécurité Cisco cisco-sa-20160201-apic-em du 01 février 2016<br>Bulletin de sécurité Cisco cisco-sa-20160201-fd du 01 février 2016<br>Bulletin de sécurité Cisco cisco-sa-20160127-ntpd du 27 janvier 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
- atteinte à l'intégrité des données
- injection de code indirecte à distance

## 2 - Systèmes affectés

- Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM) version 1.1
- Cisco Fog Director version 1.0(0)
- Cisco Jabber Guest 10.0(2)
- Cisco Application and Content Networking System (ACNS) versions antérieures à 5.5.41 (disponible le 29 février 2016)
- Cisco ASA CX et Cisco Prime Security Manager versions antérieures à 9.3.4.5 (disponible le 30 mai 2016)
- Cisco Clean Access Manager versions antérieures à 4.9.5 (disponible le 19 février 2016)
- Cisco FireSIGHT System Software versions antérieures à 6.1 (disponible en juin 2016)
- Cisco Intrusion Prevention System Solutions (IPS) versions antérieures à 7.1(11) Patch 1 (disponible le 31 mars 2016)
- Cisco Intrusion Prevention System Solutions (IPS) versions antérieures à 7.3(05) Patch 1 (disponible le 30 avril 2016)
- Cisco NAC Guest Server versions antérieures à 2.1.0 (disponible le 19 février 2016)

- Cisco NAC Server versions antérieures à 4.9.5 (disponible le 19 février 2016)
- Cisco UCS Central
- Cisco Virtual Topology System
- Unified Communications Deployment Tools
- Cisco 910 Industrial Router
- Cisco Application Policy Infrastructure Controller (APIC)
- Cisco Service Control Operating System
- IOS-XR for Cisco Network Convergence System (NCS) 6000
- Cisco Standalone rack server CIMC
- Cisco 3G Femtocell Wireless versions antérieures à SR10MR (disponible le 29 juillet 2016)
- Cisco Finesse
- Cisco Hosted Collaboration Mediation Fulfillment
- Cisco IP Interoperability and Collaboration System (IPICS)
- Cisco Management Heartbeat Server versions antérieures à RMS5.x MR (disponible le 29 juillet 2016)
- Cisco Quantum Virtualized Packet Core
- Cisco Unified Communications Manager (UCM)
- Cisco Unified Communications Manager Session Management Edition (SME)
- Cisco DCM Series 9900-Digital Content Manager versions antérieures à 18.0 (disponible le 31 mars 2016)
- Cisco Digital Media Manager (DMM)
- Cisco Digital Media Manager
- Cisco Edge 300 Digital Media Player versions antérieures à 1.6RB4_4 (disponible le 25 février 2016)
- Cisco Enterprise Content Delivery System (ECDS) versions antérieures à 2.6.7 (disponible le 30 avril 2016)
- Cisco Expressway Series versions antérieures à 8.7.1 (disponible le 22 février 2016)
- Cisco Media Experience Engines (MXE)
- Cisco TelePresence Conductor versions antérieures à XC4.2 (disponible le 30 mars 2016)
- Cisco TelePresence EX Series
- Cisco TelePresence MX Series
- Cisco TelePresence Profile Series
- Cisco TelePresence SX Series
- Cisco TelePresence Video Communication Server (VCS) versions antérieures à 8.7.1 (disponible le 22 février 2016)
- Cisco Telepresence Integrator C Series
- Cisco Video Delivery System Recorder (correctif disponible le 30 avril 2016)
- Cisco Video Distribution Suite for Internet Streaming (VDS-IS/CDS-IS)
- Cisco Video Surveillance Media Server
- Cisco Videoscape Policy and Resource Management
- Cloud Object Store (COS) versions antérieures à 3.8 (disponible le 9 avril 2016)
- Cisco Intelligent Automation for Cloud
- Cisco Universal Small Cell 5000 Series exécutant la version V3.4.2.x
- Cisco Universal Small Cell 7000 Series exécutant la version V3.4.2.x

# 3 - Résumé

De multiples vulnérabilités ont été corrigées dans *les produits Cisco*. Elles permettent à un attaquant de provoquer un déni de service à distance, une atteinte à l'intégrité des données et une injection de code indirecte à distance (XSS).

# 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-20160201-apic-em du 01 février 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160201-apic-em
- Bulletin de sécurité Cisco cisco-sa-20160201-fd du 01 février 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160201-fd
- Bulletin de sécurité Cisco cisco-sa-20160127-ntpd du 27 janvier 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160127-ntpd
- Référence CVE CVE-2015-7973
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7973
- Référence CVE CVE-2015-7974
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7974
- Référence CVE CVE-2015-7975
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7975
- Référence CVE CVE-2015-7976
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7976
- Référence CVE CVE-2015-7977
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7977
- Référence CVE CVE-2015-7978
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7978
- Référence CVE CVE-2015-7979
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7979
- Référence CVE CVE-2015-8138
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8138
- Référence CVE CVE-2015-8139
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8139
- Référence CVE CVE-2015-8140
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8140
- Référence CVE CVE-2015-8158
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8158
- Référence CVE CVE-2016-1305
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1305
- Référence CVE CVE-2016-1306
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1306

# Gestion détaillée du document

**02 février 2016** version initiale.