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 09 février 2016
N° CERTFR-2016-AVI-051

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans les produits Cisco

Gestion du document

Référence	CERTFR-2016-AVI-051
Titre	Multiples vulnérabilités dans les produits Cisco
Date de la première version	09 février 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco cisco-sa-201600208-ucm du 09 février 2016 Bulletin de sécurité Cisco cisco-sa-20160208-ucm du 09 février 2016 Bulletin de sécurité Cisco cisco-sa-20160208-vcs du 09 février 2016 Bulletin de sécurité Cisco cisco-sa-20160208-apic du 09 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)

- contournement de la politique de sécurité
- atteinte à la confidentialité des données
- injection de code indirecte à distance

2 - Systèmes affectés

- Cisco Unified Communications Manager version 11.5(0.98000.480)
- Cisco Unified Communications Manager (CallManager) versions 10.5(2.12901.1), 10.5(2.10000.5), 11.0(1.10000.10), et 9.1(2.10000.28)
- Cisco Unified Communications Manager IM & Presence Service version 10.5(2)
- Cisco Unified Contact Center Express version 11.0(1)
- Cisco Unity Connection version 10.5(2)
- Cisco TelePresence Video Communication Server (VCS) version X8 lorsqu'utilisé dans le cadre d'un déploiement Jabber Guest
- Cisco APIC-EM version 1.1

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *les produits Cisco*. Elles permettent à un attaquant de provoquer un contournement de la politique de sécurité, une atteinte à la confidentialité 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-201600208-ucm du 09 février 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-201600208-ucm
- Bulletin de sécurité Cisco cisco-sa-20160208-ucm du 09 février 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160208-ucm
- Bulletin de sécurité Cisco cisco-sa-20160208-vcs du 09 février 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160208-vcs
- Bulletin de sécurité Cisco cisco-sa-20160208-apic du 09 février 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160208-apic
- Référence CVE CVE-2016-1317
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1317
- Référence CVE CVE-2016-1319
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1319
- Référence CVE CVE-2016-1316
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1316
- Référence CVE CVE-2016-1318
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1318

Gestion détaillée du document

09 février 2016 version initiale.