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 14 avril 2016
N° CERTFR-2016-AVI-129

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans les produits Cisco

Gestion du document

Référence	CERTFR-2016-AVI-129
Titre	Multiples vulnérabilités dans les produits Cisco
Date de la première version	14 avril 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco cisco-sa-20160413-ucs du 13 avril 2016 Bulletin de sécurité Cisco cisco-sa-20160413-nms du 13 avril 2016 Bulletin de sécurité Cisco cisco-sa-20160412-unity du 12 avril 2016 Bulletin de sécurité Cisco cisco-sa-20160412-asr du 12 avril 2016 Bulletin de sécurité Cisco cisco-sa-20160407-cic du 7 avril 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
- injection de code indirecte à distance

2 - Systèmes affectés

- Cisco UCS Central Software versions antérieures à 1.3(1c)
- Cisco IOS versions antérieures à 15.2(2)E1
- Cisco Unity Connection versions 11.0 et antérieures
- Cisco IOS XR versions 4.2.3, 4.3.0, 4.3.4, et 5.3.1 s'exécutant sur les routeurs à services d'agrégation Cisco séries ASR 9000
- Cisco IP Interoperability and Collaboration System version 4.10(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-20160413-ucs du 13 avril 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160413-ucs
- Bulletin de sécurité Cisco cisco-sa-20160413-nms du 13 avril 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160413-nms
- Bulletin de sécurité Cisco cisco-sa-20160412-unity du 12 avril 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160412-unity
- Bulletin de sécurité Cisco cisco-sa-20160412-asr du 12 avril 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160412-asr
- Bulletin de sécurité Cisco cisco-sa-20160407-cic du 7 avril 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160407-cic
- Référence CVE CVE-2016-1352
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1352
- Référence CVE CVE-2016-1375
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1375
- Référence CVE CVE-2016-1376
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1376
- Référence CVE CVE-2016-1377
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1377
- Référence CVE CVE-2016-1378
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1378

Gestion détaillée du document

14 avril 2016 version initiale.