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 22 septembre 2016
N° CERTFR-2016-AVI-318

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans les produits Cisco

Gestion du document

Référence	CERTFR-2016-AVI-318
Titre	Multiples vulnérabilités dans les produits Cisco
Date de la première version	22 septembre 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco cisco-sa-20160921-csp2100-1 du 21 septembre 2016 Bulletin de sécurité Cisco cisco-sa-20160921-csp2100-2 du 21 septembre 2016 Bulletin de sécurité Cisco cisco-sa-20160921-apic du 21 septembre 2016 Bulletin de sécurité Cisco cisco-sa-20160921-caf du 21 septembre 2016 Bulletin de sécurité Cisco cisco-sa-20160921-caf1 du 21 septembre 2016 Bulletin de sécurité Cisco cisco-sa-20160921-cph du 21 septembre 2016 Bulletin de sécurité Cisco cisco-sa-20160921-dmo du 21 septembre 2016 Bulletin de sécurité Cisco cisco-sa-20160921-fmc du 21 septembre 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)

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

2 - Systèmes affectés

- Cisco Cloud Services Platform 2100 version 2.0
- Cisco Application Policy Infrastructure Controller (APIC)
- Cisco IOS et IOS XE avec la fonctionnalité IOx activée
- Cisco Prime Home
- Cisco Firepower Management Center and Cisco FireSIGHT System

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-20160921-csp2100-1 du 21 septembre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160921-csp2100-1
- Bulletin de sécurité Cisco cisco-sa-20160921-csp2100-2 du 21 septembre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160921-csp2100-2
- Bulletin de sécurité Cisco cisco-sa-20160921-apic du 21 septembre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160921-apic
- Bulletin de sécurité Cisco cisco-sa-20160921-caf du 21 septembre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160921-caf
- Bulletin de sécurité Cisco cisco-sa-20160921-caf1 du 21 septembre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160921-caf1
- Bulletin de sécurité Cisco cisco-sa-20160921-cph du 21 septembre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160921-cph
- Bulletin de sécurité Cisco cisco-sa-20160921-dmo du 21 septembre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160921-dmo
- Bulletin de sécurité Cisco cisco-sa-20160921-fmc du 21 septembre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160921-fmc
- Référence CVE CVE-2016-6373
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6373
- Référence CVE CVE-2016-6374
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6374
- Référence CVE CVE-2016-6408
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6408
- Référence CVE CVE-2016-6409
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6409
- Référence CVE CVE-2016-6410
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6410
- Référence CVE CVE-2016-6411
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6411
- Référence CVE CVE-2016-6412
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6412
- Référence CVE CVE-2016-6413
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6413

Gestion détaillée du document

22 septembre 2016 version initiale.