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 15 mars 2017
N° CERTFR-2017-AVI-084

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans les produits Cisco

Gestion du document

Référence	CERTFR-2017-AVI-084
Titre	Multiples vulnérabilités dans les produits Cisco
Date de la première version	15 mars 2017
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco cisco-sa-20170315-wlc-mesh du 15 mars 2017 Bulletin de sécurité Cisco cisco-sa-20170315-tes du 15 mars 2017 Bulletin de sécurité Cisco cisco-sa-20170315-asr du 15 mars 2017 Bulletin de sécurité Cisco cisco-sa-20170315-ap1800 du 15 mars 2017
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
- élévation de privilèges

2 - Systèmes affectés

- Cisco 8500 Series Wireless Controller
- Cisco 5500 Series Wireless Controller
- Cisco 2500 Series Wireless Controller
- Cisco Flex 7500 Series Wireless Controller
- Cisco Virtual Wireless Controller
- Wireless Services Module 2 (WiSM2)
- Cisco Tidal Enterprise Scheduler Client Manager Server versions 6.2.1.435 et postérieures
- Cisco Workload Automation Client Manager Server versions 6.3.0.116 et postérieures
- Cisco Mobility Express 1800 Series Access Points avec une version logicielle antérieure à 8.2.110.0
- Cisco ASR 5000/5500/5700 Series avec StarOS versions postérieures à 17.7.0 et antérieures à 18.7.4, 19.5, ou 20.2.3 avec SSH
- Cisco Virtualized Packet Core avec StarOS versions antérieures à N 4.2.7 (19.3.v7) et N4.7 (20.2.v0) avec SSH

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 élévation de privilèges.

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-20170315-wlc-mesh du 15 mars 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170315-wlc-mesh
- Bulletin de sécurité Cisco cisco-sa-20170315-tes du 15 mars 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170315-tes
- Bulletin de sécurité Cisco cisco-sa-20170315-asr du 15 mars 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170315-asr
- Bulletin de sécurité Cisco cisco-sa-20170315-ap1800 du 15 mars 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170315-ap1800
- Référence CVE CVE-2017-3819
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3819
- Référence CVE CVE-2017-3846
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3846
- Référence CVE CVE-2017-3854
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3854
- Référence CVE CVE-2017-3831
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3831

Gestion détaillée du document

15 mars 2017 version initiale.