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 04 mai 2017
N° CERTFR-2017-AVI-139

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans les produits Cisco

Gestion du document

Référence	CERTFR-2017-AVI-139
Titre	Multiples vulnérabilités dans les produits Cisco
Date de la première version	04 mai 2017
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco cisco-sa-20170503-cvr100w1 du 03 mai 2017 Bulletin de sécurité Cisco cisco-sa-20170503-cme du 03 mai 2017 Bulletin de sécurité Cisco cisco-sa-20170503-ctp du 03 mai 2017 Bulletin de sécurité Cisco cisco-sa-20170503-ios-xr du 03 mai 2017 Bulletin de sécurité Cisco cisco-sa-20170503-cvr100w2 du 03 mai 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)

- exécution de code arbitraire à distance
- déni de service à distance
- contournement de la politique de sécurité
- élévation de privilèges

2 - Systèmes affectés

- Cisco CVR100W Wireless-N VPN Router versions antérieures à 1.0.1.24
- Cisco Aironet 1800, 2800, 3800 Access Points versions 8.3.x antérieures à 8.3.112.0
- Cisco TelePresence Collaboration Endpoint (CE) versions antérieures à 8.3.2
- Cisco IOS XR versions 6.1.x antérieures à 6.1.2

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-20170503-cvr100w1 du 03 mai 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170503-cvr100w1
- Bulletin de sécurité Cisco cisco-sa-20170503-cme du 03 mai 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170503-cme
- Bulletin de sécurité Cisco cisco-sa-20170503-ctp du 03 mai 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170503-ctp
- Bulletin de sécurité Cisco cisco-sa-20170503-ios-xr du 03 mai 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170503-ios-xr
- Bulletin de sécurité Cisco cisco-sa-20170503-cvr100w2 du 03 mai 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170503-cvr100w2
- Référence CVE CVE-2017-3882
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3882
- Référence CVE CVE-2017-3873
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3873
- Référence CVE CVE-2017-3825
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3825
- Référence CVE CVE-2017-3876
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3876
- Référence CVE CVE-2017-6620
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6620

Gestion détaillée du document

04 mai 2017 version initiale.