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 août 2016
N° CERTFR-2016-AVI-260

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans les produits Cisco

Gestion du document

Référence	CERTFR-2016-AVI-260
Titre	Multiples vulnérabilités dans les produits Cisco
Date de la première version	04 août 2016
Date de la dernière version	05 août 2016
Source(s)	Bulletin de sécurité Cisco cisco-sa-20160803-rv110 130w2 du 03 août 2016 Bulletin de sécurité Cisco cisco-sa-20160804-wedge du 04 août 2016 Bulletin de sécurité Cisco cisco-sa-20160803-ucm du 03 août 2016 Bulletin de sécurité Cisco cisco-sa-20160803-cpi du 03 août 2016 Bulletin de sécurité Cisco cisco-sa-20160803-vcse du 03 août 2016 Bulletin de sécurité Cisco cisco-sa-20160803-rv110 130w1 du 03 août 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

2 - Systèmes affectés

- Cisco RV110W Wireless-N VPN Firewall versions antérieures à 1.2.1.7
- Cisco RV130W Wireless-N Multifunction VPN Router versions antérieures à 1.0.3.16
- Cisco RV215W Wireless-N VPN Router versions antérieures à 1.0.3.8
- Cisco IOS versions antérieures à 15.6(3)M
- Cisco IOS versions antérieures à 15.6(2)SP
- Cisco Prime Infrastructure Release 2.2(2)
- Cisco Unified Communications Manager IM and Presence Service versions antérieures à 11.5(1) SU1
- Cisco Unified Communications Manager IM and Presence Service version 11.0(1) sans le correctif de sécurité ciscocm.cup-psirt-sipd-1101-v1.1.cop.sgn

- Cisco Unified Communications Manager IM and Presence Service version 10.5(2) sans le correctif de sécurité ciscocm.cup-psirt-sipd-1052-v1.1.cop.sgn
- Cisco Unified Communications Manager IM and Presence Service version 9.1(1) sans le correctif de sécurité ciscocm.cup-psirt-sipd-911SU-v1.1.cop.sgn
- Cisco TelePresence Video Communication Server Expressway version X8.5.2

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *les produits Cisco*. 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-20160803-rv110_130w2 du 03 août 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160803-rv110_130w2
- Bulletin de sécurité Cisco cisco-sa-20160804-wedge du 04 août 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160804-wedge
- Bulletin de sécurité Cisco cisco-sa-20160803-ucm du 03 août 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160803-ucm
- Bulletin de sécurité Cisco cisco-sa-20160803-cpi du 03 août 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160803-cpi
- Bulletin de sécurité Cisco cisco-sa-20160803-vcse du 03 août 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160803-vcse
- Bulletin de sécurité Cisco cisco-sa-20160803-rv110_130w1 du 03 août 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160803-rv110_130w1
- Annonce d'arrêt de commercialisation et de fin de vie des routeurs VPN Cisco RV180
  http://www.cisco.com/c/en/us/products/collateral/routers/small-business-rv-series-routers/eos-eol-notice-c51-733327-fr.html
- Annonce d'arrêt de commercialisation et de fin de vie des routeurs VPN multifonction pour réseaux sans fil Cisco RV180W
  http://www.cisco.com/c/en/us/products/collateral/routers/small-business-rv-series-routers/eos-eol-notice-c51-733326-fr.html
- Référence CVE CVE-2015-6397
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6397
- Référence CVE CVE-2016-1466
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1466
- Référence CVE CVE-2016-1474
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1474
- Référence CVE CVE-2016-1468
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1468
- Référence CVE CVE-2015-6396
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6396
- Référence CVE CVE-2016-1478
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1478

Gestion détaillée du document

04 août 2016 version initiale.
05 août 2016 ajout du bulletin de sécurité Cisco cisco-sa-20160804-wedge