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 16 juin 2016
N° CERTFR-2016-AVI-209

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans les produits Cisco

Gestion du document

Référence	CERTFR-2016-AVI-209
Titre	Multiples vulnérabilités dans les produits Cisco
Date de la première version	16 juin 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco cisco-sa-20160615-rv du 15 juin 2016 Bulletin de sécurité Cisco cisco-sa-20160615-rv1 du 15 juin 2016 Bulletin de sécurité Cisco cisco-sa-20160615-rv2 du 15 juin 2016 Bulletin de sécurité Cisco cisco-sa-20160615-rv3 du 15 juin 2016 Bulletin de sécurité Cisco cisco-sa-20160609-ipp du 09 juin 2016 Bulletin de sécurité Cisco cisco-sa-20160609-apic du 09 juin 2016 Bulletin de sécurité Cisco cisco-sa-20160608-aironet du 09 juin 2016 Bulletin de sécurité Cisco cisco-sa-20160606-aap du 06 juin 2016 Bulletin de sécurité Cisco cisco-sa-20160603-ipp du 03 juin 2016 Bulletin de sécurité Cisco cisco-sa-20160603-ntpd du 03 juin 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
- élévation de privilèges
- injection de code indirecte à distance

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 1.3.0.8
- Téléphones Cisco IP Phone 8800 Series version 11.0(1)

- Cisco Application Policy Infrastructure Controller (APIC) Software versions antérieures à 1.3(2f)
- Plateformes Cisco Access Point exécutant le logiciel version 8.2(102.43)
- Cisco Aironet 1830e Access Point exécutant le logiciel Cisco Aironet Access Point versions antérieures à 8.2(110.0)
- Cisco Aironet 1830i Access Point exécutant le logiciel Cisco Aironet Access Point versions antérieures à 8.2(110.0)
- Cisco Aironet 1850e Access Point exécutant le logiciel Cisco Aironet Access Point versions antérieures à 8.2(110.0)
- Cisco Aironet 1850i Access Point exécutant le logiciel Cisco Aironet Access Point versions antérieures à 8.2(110.0)
- Cisco Aironet 2800 Series Access Point exécutant le logiciel Cisco Aironet Access Point versions antérieures à 8.2(110.0)
- Cisco Aironet 3800 Series Access Point exécutant le logiciel Cisco Aironet Access Point versions antérieures à 8.2(110.0)

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-20160615-rv du 15 juin 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160615-rv
- Bulletin de sécurité Cisco cisco-sa-20160615-rv1 du 15 juin 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160615-rv1
- Bulletin de sécurité Cisco cisco-sa-20160615-rv2 du 15 juin 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160615-rv2
- Bulletin de sécurité Cisco cisco-sa-20160615-rv3 du 15 juin 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160615-rv3
- Bulletin de sécurité Cisco cisco-sa-20160609-ipp du 09 juin 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160609-ipp
- Bulletin de sécurité Cisco cisco-sa-20160609-apic du 09 juin 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160609-apic
- Bulletin de sécurité Cisco cisco-sa-20160608-aironet du 09 juin 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160608-aironet
- Bulletin de sécurité Cisco cisco-sa-20160606-aap du 06 juin 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160606-aap
- Bulletin de sécurité Cisco cisco-sa-20160603-ipp du 03 juin 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160603-ipp
- Bulletin de sécurité Cisco cisco-sa-20160603-ntpd du 03 juin 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160603-ntpd
- Référence CVE CVE-2016-1395
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1395
- Référence CVE CVE-2016-1396
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1396
- Référence CVE CVE-2016-1397
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1397

- Référence CVE CVE-2016-1398
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1398
- Référence CVE CVE-2016-1403
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1403
- Référence CVE CVE-2016-1418
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1418
- Référence CVE CVE-2016-1419
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1419
- Référence CVE CVE-2016-1420
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1420
- Référence CVE CVE-2016-1421
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1421
- Référence CVE CVE-2016-4953
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4953
- Référence CVE CVE-2016-4954
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4954
- Référence CVE CVE-2016-4955
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4955
- Référence CVE CVE-2016-4956
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4956
- Référence CVE CVE-2016-4957
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4957

Gestion détaillée du document

16 juin 2016 version initiale.