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 06 octobre 2016
N° CERTFR-2016-AVI-331

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans les produits Cisco

Gestion du document

Référence	CERTFR-2016-AVI-331
Titre	Multiples vulnérabilités dans les produits Cisco
Date de la première version	06 octobre 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco cisco-sa-20161005-asa-dhcp du 05 octobre 2016 Bulletin de sécurité Cisco cisco-sa-20161005-bgp du 05 octobre 2016 Bulletin de sécurité Cisco cisco-sa-20161005-catalyst du 05 octobre 2016 Bulletin de sécurité Cisco cisco-sa-20161005-chs du 05 octobre 2016 Bulletin de sécurité Cisco cisco-sa-20161005-dhcp1 du 05 octobre 2016 Bulletin de sécurité Cisco cisco-sa-20161005-dhcp2 du 05 octobre 2016 Bulletin de sécurité Cisco cisco-sa-20161005-ftmc du 05 octobre 2016 Bulletin de sécurité Cisco cisco-sa-20161005-ftmc1 du 05 octobre 2016 Bulletin de sécurité Cisco cisco-sa-20161005-ftmc2 du 05 octobre 2016 Bulletin de sécurité Cisco cisco-sa-20161005-ios-ikev du 05 octobre 2016 Bulletin de sécurité Cisco cisco-sa-20161005-iosxr du 05 octobre 2016 Bulletin de sécurité Cisco cisco-sa-20161005-n9kinfo du 05 octobre 2016 Bulletin de sécurité Cisco cisco-sa-20161005-nxaaa du 05 octobre 2016 Bulletin de sécurité Cisco cisco-sa-20161005-otv du 05 octobre 2016 Bulletin de sécurité Cisco cisco-sa-20161005-ucis1 du 05 octobre 2016 Bulletin de sécurité Cisco cisco-sa-20161005-ucis2 du 05 octobre 2016 Bulletin de sécurité Cisco cisco-sa-20161005-ucis3 du 05 octobre 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

De multiples produits sont impactés. Se référer au bulletin de l'éditeur pour la liste exhaustive des produits.

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-20161005-asa-dhcp du 05 octobre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161005-asa-dhcp
- Bulletin de sécurité Cisco cisco-sa-20161005-bgp du 05 octobre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161005-bgp
- Bulletin de sécurité Cisco cisco-sa-20161005-catalyst du 05 octobre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161005-catalyst
- Bulletin de sécurité Cisco cisco-sa-20161005-chs du 05 octobre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161005-chs
- Bulletin de sécurité Cisco cisco-sa-20161005-dhcp1 du 05 octobre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161005-dhcp1
- Bulletin de sécurité Cisco cisco-sa-20161005-dhcp2 du 05 octobre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161005-dhcp2
- Bulletin de sécurité Cisco cisco-sa-20161005-ftmc du 05 octobre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161005-ftmc
- Bulletin de sécurité Cisco cisco-sa-20161005-ftmc1 du 05 octobre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161005-ftmc1
- Bulletin de sécurité Cisco cisco-sa-20161005-ftmc2 du 05 octobre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161005-ftmc2
- Bulletin de sécurité Cisco cisco-sa-20161005-ios-ikev du 05 octobre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161005-ios-ikev
- Bulletin de sécurité Cisco cisco-sa-20161005-iosxr du 05 octobre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161005-iosxr
- Bulletin de sécurité Cisco cisco-sa-20161005-n9kinfo du 05 octobre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161005-n9kinfo
- Bulletin de sécurité Cisco cisco-sa-20161005-nxaaa du 05 octobre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161005-nxaaa
- Bulletin de sécurité Cisco cisco-sa-20161005-otv du 05 octobre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161005-otv
- Bulletin de sécurité Cisco cisco-sa-20161005-ucis1 du 05 octobre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161005-ucis1
- Bulletin de sécurité Cisco cisco-sa-20161005-ucis2 du 05 octobre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161005-ucis2
- Bulletin de sécurité Cisco cisco-sa-20161005-ucis3 du 05 octobre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161005-ucis3
- Référence CVE CVE-2016-6424
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6424
- Référence CVE CVE-2016-1454
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1454

- Référence CVE CVE-2016-6422
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6422
- Référence CVE CVE-2016-6436
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6436
- Référence CVE CVE-2015-6392
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6392
- Référence CVE CVE-2015-6393
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6393
- Référence CVE CVE-2016-6433
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6433
- Référence CVE CVE-2016-6434
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6434
- Référence CVE CVE-2016-6435
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6435
- Référence CVE CVE-2016-6423
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6423
- Référence CVE CVE-2016-6428
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6428
- Référence CVE CVE-2016-1455
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1455
- Référence CVE CVE-2015-0721
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0721
- Référence CVE CVE-2016-1453
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1453
- Référence CVE CVE-2016-6425
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6425
- Référence CVE CVE-2016-6426
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6426
- Référence CVE CVE-2016-6427
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6427

Gestion détaillée du document

06 octobre 2016 version initiale.