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 29 septembre 2016
N° CERTFR-2016-AVI-322

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans Cisco IOS et IOS XE

Gestion du document

Référence	CERTFR-2016-AVI-322
Titre	Multiples vulnérabilités dans Cisco IOS et IOS XE
Date de la première version	29 septembre 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco cisco-sa-20160928-smi du 28 septembre 2016 Bulletin de sécurité Cisco cisco-sa-20160928-msdp du 28 septembre 2016 Bulletin de sécurité Cisco cisco-sa-20160928-ipdr du 28 septembre 2016 Bulletin de sécurité Cisco cisco-sa-20160928-ios-ikev1 du 28 septembre 2016 Bulletin de sécurité Cisco cisco-sa-20160928-h323 du 28 septembre 2016 Bulletin de sécurité Cisco cisco-sa-20160928-frag du 28 septembre 2016 Bulletin de sécurité Cisco cisco-sa-20160928-dns du 28 septembre 2016 Bulletin de sécurité Cisco cisco-sa-20160928-cip du 28 septembre 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)

- déni de service
- atteinte à la confidentialité des données

2 - Systèmes affectés

- Cisco IOS XE versions 3.x
- Cisco IOS XE versions 16.x
- Cisco IOS, voir sur le site du constructeur pour vérifier si votre système est vulnérable (cf. section Documentation)

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *Cisco IOS* et *Cisco IOS XE*. Elles permettent à un attaquant de provoquer un déni de service et une atteinte à la confidentialité des données.

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-20160928-smi du 28 septembre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160928-smi
- Bulletin de sécurité Cisco cisco-sa-20160928-msdp du 28 septembre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160928-msdp
- Bulletin de sécurité Cisco cisco-sa-20160928-ipdr du 28 septembre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160928-ipdr
- Bulletin de sécurité Cisco cisco-sa-20160928-ios-ikev1 du 28 septembre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160928-ios-ikev1
- Bulletin de sécurité Cisco cisco-sa-20160928-h323 du 28 septembre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160928-h323
- Bulletin de sécurité Cisco cisco-sa-20160928-frag du 28 septembre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160928-frag
- Bulletin de sécurité Cisco cisco-sa-20160928-dns du 28 septembre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160928-dns
- Bulletin de sécurité Cisco cisco-sa-20160928-cip du 28 septembre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160928-cip
- Référence CVE CVE-2016-6379
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6379
- Référence CVE CVE-2016-6380
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6380
- Référence CVE CVE-2016-6381
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6381
- Référence CVE CVE-2016-6382
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6382
- Référence CVE CVE-2016-6384
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6384
- Référence CVE CVE-2016-6385
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6385
- Référence CVE CVE-2016-6386
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6386
- Référence CVE CVE-2016-6391
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6391

Gestion détaillée du document

29 septembre 2016 version initiale.