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 15 septembre 2016
N° CERTFR-2016-AVI-312

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans les produits Cisco

Gestion du document

Référence	CERTFR-2016-AVI-312
Titre	Multiples vulnérabilités dans les produits Cisco
Date de la première version	15 septembre 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco cisco-sa-20160914-wem du 14 septembre 2016 Bulletin de sécurité Cisco cisco-sa-20160914-wms du 14 septembre 2016 Bulletin de sécurité Cisco cisco-sa-20160914-ios du 14 septembre 2016 Bulletin de sécurité Cisco cisco-sa-20160914-ios-xe du 14 septembre 2016 Bulletin de sécurité Cisco cisco-sa-20160914-iosxr du 14 septembre 2016 Bulletin de sécurité Cisco cisco-sa-20160914-ioxfd du 14 septembre 2016 Bulletin de sécurité Cisco cisco-sa-20160907-fsss du 7 septembre 2016 Bulletin de sécurité Cisco cisco-sa-20160907-fsss1 du 7 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)

- exécution de code arbitraire à distance
- déni de service à distance
- contournement de la politique de sécurité
- atteinte à l'intégrité des données
- injection de code indirecte à distance

2 - Systèmes affectés

- Cisco WebEx Meetings Server version 2.6
- Cisco IOS et IOS XE Software IOx Local Manager
- Cisco Fog Director pour IOx
- Cisco Firepower Management Center versions antérieures à 6.1
- Cisco FireSIGHT System Software versions antérieures à 6.1

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-20160914-wem du 14 septembre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160914-wem
- Bulletin de sécurité Cisco cisco-sa-20160914-wms du 14 septembre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160914-wms
- Bulletin de sécurité Cisco cisco-sa-20160914-ios du 14 septembre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160914-ios
- Bulletin de sécurité Cisco cisco-sa-20160914-ios-xe du 14 septembre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160914-ios-xe
- Bulletin de sécurité Cisco cisco-sa-20160914-iosxr du 14 septembre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160914-iosxr
- Bulletin de sécurité Cisco cisco-sa-20160914-ioxfd du 14 septembre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160914-ioxfd
- Bulletin de sécurité Cisco cisco-sa-20160907-fsss du 7 septembre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160907-fsss
- Bulletin de sécurité Cisco cisco-sa-20160907-fsss1 du 7 septembre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160907-fsss1
- Référence CVE CVE-2016-1433
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1433
- Référence CVE CVE-2016-1482
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1482
- Référence CVE CVE-2016-1483
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1483
- Référence CVE CVE-2016-6395
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6395
- Référence CVE CVE-2016-6396
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6396
- Référence CVE CVE-2016-6403
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6403
- Référence CVE CVE-2016-6404
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6404
- Référence CVE CVE-2016-6405
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6405

Gestion détaillée du document

15 septembre 2016 version initiale.

Conditions d'utilisation de ce document : http://cert.ssi.gouv.fr/cert-fr/apropos.html
Dernière version de ce document : http://cert.ssi.gouv.fr/site/CERTFR-2016-AVI-312